

Linear Information Coupling Problems

Shao-Lun Huang and Lizhong Zheng

Abstract

Many network information theory problems face the similar difficulty of single-letterization. We argue that this is due to the lack of a geometric structure on the space of probability distribution. In this paper, we develop such a structure by assuming that the distributions of interest are close to each other. Under this assumption, the K-L divergence is reduced to the squared Euclidean metric in an Euclidean space. In addition, we construct the notion of coordinate and inner product, which will facilitate solving communication problems. We will present the application of this approach to the point-to-point channel, general broadcast channel, and the multiple access channel (MAC) with the common source. It can be shown that with this approach, information theory problems, such as the single-letterization, can be reduced to some linear algebra problems. Moreover, we show that for the general broadcast channel, transmitting the common message to receivers can be formulated as the trade-off between linear systems. We also provide an example to visualize this trade-off in a geometric way. Finally, for the MAC with the common source, we observe a coherent combining gain due to the cooperation between transmitters, and this gain can be quantified by applying our technique.

Index Terms

Information Geometry, Local Approximation, Divergence Transition Matrix (DTM), Euclidean Information Theory, Kullback-Leiber divergence

I. INTRODUCTION

In this paper, we study a certain class of information theory problems for discrete memoryless communication networks, which we call the *linear information coupling problems*. For a communication network, the corresponding linear information coupling problem asks the question that how we can efficiently transmit a thin layer of information through this network. More rigorously, we assume that there are sequences of input symbols generated at each transmitter from an i.i.d. distribution P_X . We also assume that the network is composed of some discrete memoryless channels, whose outputs are sequences with an i.i.d. distribution P_Y . We take this setup as an operating point. To encode an information $U = u$, we alter some of these input symbols, such that the empirical distribution changes to $P_{X|U=u}$. We insist that for each u , $P_{X|U=u}$ is close to P_X , which means we can only alter a small fraction of the input symbols. Moreover, when averaging over all different values of u , the marginal distribution of X remains unchanged. The receivers can then decode the information by distinguishing empirical output distributions with respect to different u . The goal of the linear information coupling problem is to design $P_{X|U=u}$ for different u , such that the receivers can distinguish different empirical output distributions the most efficiently. Mathematically, for the point-to-point channel with input X and output Y , the linear information coupling problem of this channel can be formulated as the multi-letter problem: for a given pair of input and output sequences X^n, Y^n , with joint distribution

$$P_{X^n Y^n}(x^n, y^n) = \prod_{i=1}^n P_X(x_i) \cdot P_{Y|X}(y_i|x_i)$$

we consider the problem

$$\max_{U \rightarrow X^n \rightarrow Y^n} \frac{1}{n} I(U; Y^n), \quad (1)$$

$$\text{subject to: } \frac{1}{n} I(U; X^n) \leq \delta, \quad (2)$$

$$\frac{1}{n} \|P_{X^n|U=u} - P_{X^n}\|^2 = O(\delta), \quad \forall u, \quad (3)$$

where δ is the amount of information modulated in per input symbol X , and is assumed to be small. Here, both $P_{X^n|U=u}$ and P_{X^n} in (3) are viewed as $|\mathcal{X}|^n$ dimensional vectors, and the norm square is simply the Euclidean metric.

In fact, the problem (1) is almost the same as the traditional capacity problem

$$\max_{U \rightarrow X^n \rightarrow Y^n} \frac{1}{n} I(U; Y^n), \quad (4)$$

where U is the message transmitted through the channel. This traditional problem has the solution $\max_{P_X} I(X; Y)$ [1]. The difference between (4) and (1) lies in the constraint (2) and (3). Somewhat surprisingly, we will show that with these differences, the linear information coupling problem (1) can be solved quite differently from the corresponding capacity problem (4).

The linear information coupling problem (1) indeed captures some fundamental aspects of the traditional capacity problem. We will demonstrate in section II that the problem (1) is a sub-problem of the capacity problem. In general, the problem (1) is a local version of the global optimization problem (4), and the solutions of (1) are local optimal solutions of the corresponding capacity problem. In addition, we can “integral” the solutions of a set of linear information coupling problems back to a solution of the capacity problem.

One important feature of the linear information coupling problems is that when the local assumptions (2) and (3) are added to the problem, there is a systematic approach for single-letterization for general multi-terminal communication problems. We first demonstrate in section II-B that, with a simple linear algebra technique, the linear information coupling problem (1) can be single-letterized to its single-letter version

$$\begin{aligned} & \max_{U \rightarrow X \rightarrow Y} I(U; Y), \\ & \text{subject to: } I(U; X) \leq \delta, \\ & \|P_{X|U=u} - P_X\|^2 = O(\delta), \quad \forall u, \end{aligned} \tag{5}$$

where U follows the common cardinality bounds. Then, we illustrate in section III and IV that for general multi-terminal communication problems, the single-letterization procedure is conceptually the same as the point-to-point channel case. Note that the single-letterization is precisely the difficulty to generalize the conventional capacity results on the point-to-point channels to general multi-terminal problems, this systematic procedure for the linear information coupling problems thus makes these problems particularly attractive.

The main reason that allows this much simpler procedure of single-letterization is that the locality assumptions (2) and (3) fundamentally simplifies the geometric structure of the space of probability distributions. In a nutshell, it allows us to approximate the manifold structure of this space [4] by its linear tangent plane. Put it another way, if we view a 1-dimensional family of probability distributions as a parameterized curve in the space of distributions, the locality assumption allows us to focus only on “straight lines”, and further approximate the Fisher information w.r.t. the underlying parameter as a constant along the curve. Such simplification, under different names, has been taken advantage of in several different areas, to produce often the cleanest results, including efficient parameter estimation with large samples, error exponent for very-noisy channels, etc. In the literature of information theory, the work on differential efficiency on investments, by Erkip and Cover [8], which was based on Rényi’s formulation of maximal correlation [12], is one of such examples. Some of the connections between these results will be discussed in this paper.

Mathematically, the locality assumption manifests into a quadratic approximation to the Kullback-Leibler (K-L) divergence. When the conditional distributions $P_{X|U=u}$ are close to the empirical distribution P_X for all u , we can approximate the K-L divergence $D(P_{X|U=u} || P_X)$, and hence the mutual information $I(U; X)$, by quadratic functions, which turns out to be related to the Euclidean distance between these two distributions. With this local approximation, the space of the input distributions is locally approximated as an Euclidean space around P_X . Similarly, the space of the output distributions can also be locally approximated as an Euclidean space around P_Y . We can construct geometric structures in these Euclidean spaces, such as orthonormal bases and inner products. Moreover, it can be shown that the channel behaves as a linear map between the input and output Euclidean spaces. Our purpose is to find the directions to perturb from P_X , according to the information $U = u$ to be encoded, in the input distribution space; or equivalently, to design $P_{X|U=u} - P_X$, such that after the channel map, the image of this perturbation at the output distribution space is as large as possible. This turns out to be a linear algebra problem for which even the multi-letter problem can be solved analytically.

It is worth pointing out that the example on the point-to-point channel, where we linearize the map from the space of distributions on X to that on Y , is *not* where the power of this local approximation approach lies. In fact, it is well-known that for both the problem without any locality constraint, and that only has (2) but not (3), can be solved and shown to have single-letter optimal solutions. One can argue that both of these two versions of single-letterization require to establish more involved techniques, and are therefore stronger results than the linear coupling problems. However, these techniques do not generalize easily to multi-terminal problems. In contrast, our solutions to the linear coupling problems can be generalized rather easily. In this paper, we demonstrate this by applying our approach to the general broadcast channels, and show that the localized version of the problem, while does not answer the question of “capacity region”, still can offer insights to the code designs. By doing this, we also point out that the key difficulty of the classical studies on network capacities indeed lies on the non-linear nature of the space of probability distributions, or in other words, the fact that the locality constraint (3) is not used.

The rest of this paper is organized as follows. In section II, we study the linear information coupling problems for point-to-point channels. We first introduce the notion of local approximation, and show that the K-L divergence can be approximated as the squared Euclidean metric. Then, the single-letter version of the linear information coupling problems will be solved by exploiting the local geometric structure. Moreover, the single-letterization of the linear information coupling problems will be shown to be equivalent to simple linear algebra problems. We will discuss the relation between our work and the capacity results and code designs in section II-D, and the relation to the Rényi maximal correlation in section II-E. Section III is dedicated in applying the local approach to the general broadcast channels. It will be shown that the linear information coupling problems

of general broadcast channels are different from that for the point-to-point channels in general: the single-letter solutions are not optimal, however finite-letter optimal solutions always exist. The application of the local approach to the multiple access channels with common sources is presented in section IV. We show that there are coherent combining gains in transmitting the common sources, and also determine the quantity of these gains. Finally, the conclusion of this paper is given in section V.

II. THE POINT-TO-POINT CHANNEL

We start with formulating and demonstrating the solutions of the linear information coupling problems for point-to-point channels. For a discrete memoryless point-to-point channel, with input $X \in \mathcal{X}$ and output $Y \in \mathcal{Y}$, where \mathcal{X} and \mathcal{Y} are finite sets, let the $|\mathcal{Y}| \times |\mathcal{X}|$ channel matrix W denote the conditional distributions corresponding to the channel. For this channel, it is known that the capacity is given by

$$\max_{P_X} I(X; Y). \quad (6)$$

This simple expression is resulted from a multi-letter problem. If we encode a message U in n -dimensional vector X^n , and decode it from the corresponding n -dimensional channel output, we can write the problem as

$$\max_{U \rightarrow X^n \rightarrow Y^n} \frac{1}{n} I(U; Y^n), \quad (7)$$

where $U \rightarrow X^n \rightarrow Y^n$ denotes a Markov relation. It turns out that for the point-to-point channel, there is a simple procedure to prove that (7) and (6) have the same maximal value [1]:

$$\begin{aligned} \frac{1}{n} I(U; Y^n) &\leq \frac{1}{n} I(X^n; Y^n) \\ &= \frac{1}{n} \sum_i H(Y_i | Y_1^{i-1}) - H(Y_i | X^n, Y^{i-1}) \\ &\leq \frac{1}{n} \sum_i H(Y_i) - H(Y_i | X_i) \\ &= \frac{1}{n} \sum_i I(X_i; Y_i) \leq \max I(X; Y). \end{aligned} \quad (8)$$

This procedure is known as the *single-letterization*, that is, to reduce a multi-letter optimization problem to a single-letter one. It is a critical step in general capacity problems, since without such a procedure, the optimization problems can potentially be over infinite dimensional spaces, and even numerical solutions of these problems may not be possible. Unfortunately, for general multi-terminal problems, we do not have a systematic way of single-letterization, which is why many of such problems remain open. The most famous examples of such problems are the general (not degraded) broadcast channels.

In contrast to the capacity problems, we study in this paper an alternative class of problems, called linear information coupling problems. In this section, we consider the linear information coupling problems for point-to-point channels. Assume as before that X and Y are the input and output of a point-to-point channel, the linear information coupling problem of this channel is the following multi-letter optimization problem:

$$\max_{U \rightarrow X^n \rightarrow Y^n} \frac{1}{n} I(U; Y^n), \quad (9)$$

$$\text{subject to: } \frac{1}{n} I(U; X^n) \leq \delta, \quad (10)$$

$$\frac{1}{n} \|P_{X^n|U=u} - P_{X^n}\|^2 = O(\delta), \quad \forall u, \quad (11)$$

where δ is assumed to be small¹. The difference between (7) and (9) lies in the constraints (10) and (11). In the capacity problem, the entire input sequence is dedicated to encoding U ; on the other hand, for the linear information coupling problems, we can only alter the input sequence "slightly" to carry the information from U . Operationally, we assume that sequences of i.i.d. P_X distributed symbols are transmitted, and the corresponding P_Y distributed symbols are received at the channel output. This can also be viewed as having a pair of jointly distributed multi-source (X, Y) with the distribution P_{XY} . Then, we encode the message $U = u$ by altering a small number of symbols in these sequences, such that the empirical distribution changes to $P_{X|U=u}$. As we only alter a small number of symbols, the conditional distribution $P_{X|U=u}$ is close to P_X . For the rest of this paper, we assume that the marginal distribution P_{X^n} is an i.i.d. distribution over the n letters². Our goal is to find

¹In the assumption $\frac{1}{n} I(U; X^n) \leq \delta$, we implicitly assume that $\delta \ll \frac{1}{n}$, for all n , so that the approximation in section II-A will be valid for any number of letters.

²This assumption can be proved to be "without loss of the optimality" for some cases [7]. In general, it requires a separate optimization, which is not the main issue addressed in this thesis. To that end, we also assume that the given marginal P_{X^n} has strictly positive entries.

the conditional distributions $P_{X|U=u}$ for different values u , which satisfy the marginal constraint P_X , such that a thin layer of information can be conveyed to the Y end the most efficiently.

Although we assume that the operating point has i.i.d. P_X distribution, question remains on whether $P_{X^n|U=u}$ should be i.i.d.. Therefore, (9) has a multi-letter form. In fact, we will show in section II-B that, unlike the capacity problem, the linear information coupling problem allows easy single-letterization, and the optimal conditional distribution $P_{X^n|U=u}$ is indeed i.i.d.. This turns out to be a very important feature of the linear information coupling problems, since the problems are then optimized over finite dimensional spaces.

A. The Local Approximation

The key technique of our approach to solve the linear information coupling problems is to use a local approximation of the K-L divergence. Let P and Q be two distributions over the same alphabet \mathcal{X} , then $D(P\|Q) = \sum_x P(x) \log(P(x)/Q(x))$ can be viewed as a measure of distance between these two distributions. However, this distance measure is not symmetric, that is, $D(P\|Q) \neq D(Q\|P)$. The situation can be much simplified if P and Q are close. We assume that $Q(x) = P(x) + \epsilon J(x)$, for some small value ϵ , and a function $J : \mathcal{X} \mapsto \mathbb{R}$. Then, the KL divergence can be written, with the second order Taylor expansion, as

$$\begin{aligned} D(P\|Q) &= - \sum_x P(x) \log \frac{Q(x)}{P(x)} \\ &= - \sum_x P(x) \log \left(1 + \epsilon \cdot \frac{J(x)}{P(x)} \right) \\ &= \frac{1}{2} \epsilon^2 \cdot \sum_x \frac{1}{P(x)} J^2(x) + o(\epsilon^2). \end{aligned} \quad (12)$$

We think of J also as a column vector of dimension $|\mathcal{X}|$, and denote $\sum_x J^2(x)/P(x)$ as $\|J\|_P^2$, which is the weighted norm square of the perturbation vector J . It is easy to verify here that replacing the weights in this norm by $Q(x)$, or any other distribution in the neighborhood, only results in an $o(\epsilon^2)$ difference. That is, up to the first order approximation, the weights in the norm simply indicate the neighborhood of distributions where the divergence is computed. As a consequence, $D(P\|Q)$ and $D(Q\|P)$ are considered as equal up to the first order approximation.

For convenience of the notations, we define the *weighted perturbation vector* as

$$\psi(x) \triangleq \frac{1}{\sqrt{P(x)}} J(x), \quad \forall x \in \mathcal{X},$$

or in vector form $\psi \triangleq [\sqrt{P}^{-1}] J$, where $[\sqrt{P}^{-1}]$ represents the diagonal matrix with entries $\{\sqrt{P(x)}^{-1}, x \in \mathcal{X}\}$. This allows us to write $\|J\|_P^2 = \|\psi\|^2$, where the last norm is simply the Euclidean norm.

With this definition of the norm on the perturbations of distributions, we can generalize to define the corresponding notion of inner products. Let $Q_i(x) = P(x) + \epsilon \cdot J_i(x)$, $\forall x, i = 1, 2$, we can define

$$\langle J_1, J_2 \rangle_P \triangleq \sum_x \frac{1}{P(x)} J_1(x) J_2(x) = \langle \psi_1, \psi_2 \rangle,$$

where $\psi_i = [\sqrt{P}^{-1}] J_i$, for $i = 1, 2$. From this, notions of orthogonal perturbations and projections can be similarly defined. The point here is that we can view a neighborhood of distributions as a linear metric space, where each distribution Q is specified by the corresponding weighted perturbation ψ from P , and define notions of orthonormal basis and coordinates on it.

We now use this new notation to rewrite the linear information coupling problem (9), which is repeated her convenience.

$$\max_{U \rightarrow X \rightarrow Y} I(U; Y), \quad (13)$$

$$\text{subject to: } I(U; X) \leq \delta, \quad (14)$$

$$\|P_{X|U=u} - P_X\|^2 = O(\delta), \quad \forall u, \quad (15)$$

For the rest of this paper, we replace the notation δ in the constraint by $\frac{1}{2}\epsilon^2$, as in the quadratic approximation in (12). We assume that the distribution P_X is given as the operating point. The purpose of (13) is to design the distribution P_U and the conditional distributions $P_{X|U=u}$, for different values of u , to maximize the mutual information $I(U; Y)$, such that the constraint

$$I(U; X) = \sum_u P_U(u) \cdot D(P_{X|U=u} \| P_X) \leq \frac{1}{2} \epsilon^2, \quad (16)$$

is satisfied, and the marginal distribution $\sum_u P_U(u) P_{X|U=u} = P_X$. Since ϵ is small, from (16) and the local constraint (15), we

can write the conditional distributions $P_{X|U=u}$ as perturbations of P_X . Written in vector form, we have $P_{X|U=u} = P_X + \epsilon \cdot J_u$, where J_u is the perturbation vector. With the local approximation on $D(P_{X|U}(\cdot|u) \| P_X)$, the constraint (16) can be written as

$$\frac{1}{2}\epsilon^2 \sum_u P_U(u) \cdot \|J_u\|_{P_X}^2 + o(\epsilon^2) \leq \frac{1}{2}\epsilon^2,$$

which is equivalent to $\sum_u P_U(u) \cdot \|J_u\|_{P_X}^2 \leq 1$. Moreover, since the conditional distributions $P_{X|U=u}$, for different u , have to be valid probability distributions and satisfy the marginal constraint, we have the extra constraints on the perturbation vector J_u :

$$\sum_x J_u(x) = 0, \forall u, \quad (17)$$

and

$$\sum_u P_U(u) J_u(x) = 0, \forall x. \quad (18)$$

Next, for each u , let $\psi_u = [\sqrt{P_X}^{-1}] J_u$ be the weighted perturbation vector. Now, we observe that in the output distribution space

$$\begin{aligned} P_{Y|U=u} &= W P_{X|U=u} = W P_X + \epsilon \cdot W J_u \\ &= P_Y + \epsilon \cdot W [\sqrt{P_X}] \psi_u, \end{aligned}$$

where the channel applied to an input distribution is simply written as the channel matrix W , with dimension $|\mathcal{Y}| \times |\mathcal{X}|$, multiplying the input distribution as a vector. At this point, we have reduced both the spaces of input and output distributions as linear spaces, and the channel acts as a linear transform between these two spaces. The linear information coupling problem (13) can be rewritten as, ignoring the $o(\epsilon^2)$ terms:

$$\begin{aligned} &\max. \sum_u P_U(u) \cdot \|W J_u\|_{P_Y}^2, \\ &\text{subject to: } \sum_u P_U(u) \cdot \|J_u\|_{P_X}^2 = 1, \end{aligned}$$

or equivalently in terms of Euclidean norms,

$$\max. \sum_u P_U(u) \cdot \left\| [\sqrt{P_Y}^{-1}] W [\sqrt{P_X}] \cdot \psi_u \right\|^2 \quad (19)$$

$$\text{subject to: } \sum_u P_U(u) \cdot \|\psi_u\|^2 = 1. \quad (20)$$

The optimization is in the choices of ψ_u vectors, which also satisfy the constraints from (17), (18), rewritten as

$$\sum_x \sqrt{P_X(x)} \cdot \psi_u(x) = 0, \forall u \quad (21)$$

and

$$\sum_u P_U(u) \sqrt{P_X(x)} \cdot \psi_u(x) = 0, \forall x. \quad (22)$$

The problem (20) is a linear algebra problem. We need to find P_U and a corresponding weighted perturbation vectors ψ_u for every u , such that the average weighted square norm, as in (19), is maximized. For convenience, we write

$$B \triangleq [\sqrt{P_Y}^{-1}] W [\sqrt{P_X}]. \quad (23)$$

Now a simplifying observation is that in both (19) and (20) the same set of weights $P_U(u)$ are used, thus the problem can be reduced in finding a direction of ψ^* , which maximizes the ratio $\|B\psi\|/\|\psi\|$, and the optimal choice of ψ_u should be along the direction of this ψ^* for every u . From the linearity of the problem, scaling ψ_u along this direction has no effect on the result. Thus, we can with out loss of optimality pick a simple solution, with U binary equi-probable, and

$$\begin{aligned} P_{X|U=0} &= P_X + \epsilon [\sqrt{P_X}] \cdot \psi^* \\ P_{X|U=1} &= P_X - \epsilon [\sqrt{P_X}] \cdot \psi^*. \end{aligned}$$

This makes constraint (22) always satisfied.

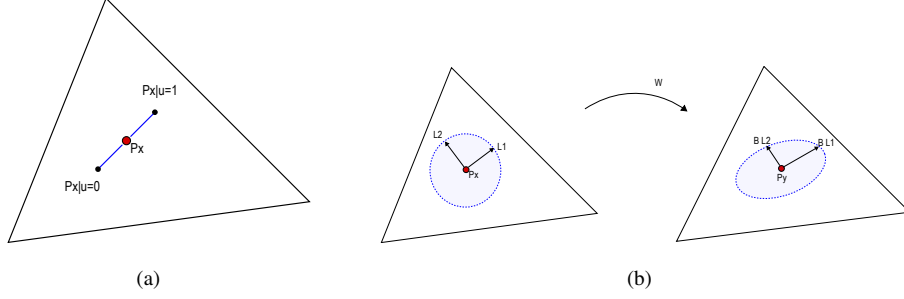


Fig. 1. (a) Choice of P_U and $P_{X|U}$ to maintain the marginal P_X . (b) Divergence Transition Map as a linear map between two spaces, with right and left singular vectors as orthonormal bases.

Figure 1(a) illustrates this idea from the geometric point of view. We rewrite the optimization problem and the constraints as:

$$\max. \quad \|B \cdot \psi\|^2, \quad (24)$$

$$\text{subject to: } \|\psi\|^2 = 1, \quad (25)$$

$$\sum_x \sqrt{P_X(x)} \psi(x) = 0. \quad (26)$$

We call this matrix B as the *divergence transition matrix* (DTM), since it maps divergence in the space of input distributions to that of the output distributions.

Now, to solve this problem, first note that if we ignore the linear constraint (26), the optimization of (24) is simply choosing ψ as the largest right (input) singular vector of B corresponding to the largest singular value. However, this choice might violate (26). We can view (26) as an orthogonality constraint between ψ and a vector $\underline{v}_0 = [\sqrt{P_X}, x \in \mathcal{X}]^T$, and still carry out the optimization. It turns out that the SVD structure of the B matrix makes this particularly simple.

Lemma 1. *Let the singular values of the DTM B be $\sigma_0 \geq \sigma_1 \geq \dots \geq \sigma_m$, with the corresponding right singular vectors $\underline{v}_0, \underline{v}_1, \dots, \underline{v}_m$, where $m = \min\{|\mathcal{X}|, |\mathcal{Y}|\} - 1$, then $\sigma_0 = 1$ and $\underline{v}_0 = [\sqrt{P_X}(x), x \in \mathcal{X}]^T$.*

Proof: First, it is easy to verify that B has a singular value of 1, corresponding to left singular vector of $\underline{w}_0 = [\sqrt{P_Y}(y), y \in \mathcal{Y}]^T$ and right singular vector \underline{v}_0 , by checking from definition that

$$B^T \cdot B \cdot \underline{v}_0 = \underline{v}_0, \quad B \cdot B^T \cdot \underline{w}_0 = \underline{w}_0$$

Observe that this \underline{v}_0 is an invalid direction to perturb distributions, in that $P_X + \epsilon[\sqrt{P_X}] \cdot \underline{v}_0$ is not a valid distribution. More importantly, any vector orthogonal to \underline{v}_0 is a valid perturbation, from (21). That is, any linear combination of the other singular vectors satisfies this constraint.

To see that all the other singular values must be no larger than 1, we consider a Markov relation $U \rightarrow X \rightarrow Y$. Let $U \sim \text{Bernoulli}(1/2)$, and

$$P_{X|U=0} = P_X + \epsilon[\sqrt{P_X}] \cdot \psi, \quad P_{X|U=1} = P_X - \epsilon[\sqrt{P_X}] \cdot \psi$$

where ψ is orthogonal to \underline{v}_0 , and hence guarantees the above are valid conditional distributions. Now from the data processing inequality, we have $I(U; Y) \leq I(U; X)$, which implies $\|B\psi\|^2 \leq \|\psi\|^2$. This shows that all other singular values of B must be no larger than 1. ■

From this lemma, we can conclude that the optimal solution to (24) is to choose ψ to be along the right singular vector of B with the second largest singular value, i.e., \underline{v}_1 .

We can visualize as in Figure 1(b) the orthonormal bases of the input and output spaces, respectively, according to the right and left singular vectors of B . The key point here is that while $I(U; X)$ measures how many bits of information is carried in X , depending on how the information is modulated, in terms of which direction the corresponding perturbation vector is, the information has different “visibility” at the receiver end. Picking the weighted perturbation vector to be along \underline{v}_1 results in the most “efficient” way to carry information through the channel.

Remark 1. The above arguments imply that

$$I(U; Y) \leq \sigma_1^2 \cdot I(U; X), \quad (27)$$

where $\sigma_1 \leq 1$ is the second largest singular value of B . Thus, comparing to the data processing inequality $I(U; Y) \leq I(U; X)$,

(27) can be viewed as a “strong data processing” inequality. Moreover, equality can be achieved if and only if for every u , $P_{X|U=u}$ differs from P_X along the weighted direction of \underline{v}_1 . If the perturbation is along other directions, then the output norm would be reduced even further according to other singular values of B . This result gives a clear view of how much information has to be lost when passing through a noisy channel.

In the literature, there are several other notions of “strong data processing inequalities”. Our result only applies to the case where the locality constraints (15) holds. Without this constraint, one can indeed find tighter bounds [16]. The point here is that the local geometric picture is indeed very clean.

Remark 2. In fact, these ideas are closely related to the method of information geometry [4], which studies the geometric structure of the space of probability distributions. In information geometry, the collection of probability distributions forms a manifold, and the K-L divergence behaves as the distance measure in this manifold. However, the K-L divergence is not symmetric, and this manifold is not flat, but has a rather complicated structure. On the other hand, our approach introduced in this subsection locally approximates this complicated manifold by a tangent hyperplane around P_X , which can be viewed as an Euclidean space, and the K-L divergence corresponds to the square norm in this linear space. For the linearized neighborhood around P_X , just like any other vector space, one can define many orthonormal bases. Here, we pick the orthonormal basis according to the SVD structure of the DTM B , which is particularly suitable as our goal is to study how much information can be coupled through this channel. This orthonormal basis illustrates the principle directions of conveying information to the receiver end under the channel map, and provides the insights of how to efficiently exploit the channel.

Remark 3. In many network information theory problems, it is required to deal with the tradeoff between multiple K-L divergence (mutual information). Even though K-L divergence is a convex function of both arguments, tradeoff, or linear combinations of multiple convex functions is no longer convex. Therefore, many of such problems are by nature non-convex optimization over potentially high dimensional spaces. This is why analytical solutions can often be hard to find.

The local approximation approach is a fundamental simplification of these problems. We approximate the K-L divergence by a quadratic function; and the tradeoff between quadratic functions remains quadratic, which is much easier to deal with. Effectively, our approach tries to find the local optima in such problems, which is a natural step when the problems are non-convex.

Remark 4. The idea of local analysis on the space of distributions is not new. In fact, it has been used in a wide range of problems, often to produce the cleanest results. One example is non-random parameter estimation [18], where asymptotically efficient estimator (achieving the Cramer-Rao bound) always exists when a large number of i.i.d. observations are available. In contrast to the non-asymptotic cases where efficient estimator does not always exists. The underlying reason of this simplicity is that the empirical distribution of a large number of i.i.d. observations lies in a small neighborhood of the true distribution, and local analysis can be employed.

The contribution of this work is to push this simplification one step further by defining an orthonormal basis on this neighborhood. As we will see in examples, this structure can be quite helpful in the analysis.

Example 1. In this example, we consider a ternary point-to-point channel with input symbols $\mathcal{X} = \{1, 2, 3\}$ and output symbols $\mathcal{Y} = \{1, 2, 3\}$ such that:

- (i) The sub-channel between the input symbols $\{2, 3\}$ and the output symbols $\{2, 3\}$ is a binary symmetric channel (BSC) with crossover probability $\frac{1}{2} - \gamma$.
- (ii) If we employ the auxiliary input/output symbol 0 to represent the transmission/receiving of the input/output symbols 2 and 3, i.e., $0 = \{2, 3\}$, then the sub-channel between the input symbols $\{0, 1\}$ and the output symbols $\{0, 1\}$ is a BSC with crossover probability $\frac{1}{2} - \eta$.

This ternary channel is illustrated in Figure 2(a). Mathematically, the channel transition matrix of this ternary channel can be specified as

$$W = \begin{bmatrix} \frac{1}{2} + \eta & \frac{1}{2} - \eta & \frac{1}{2} - \eta \\ \frac{1}{4} - \frac{1}{2}\eta & (\frac{1}{2} + \eta)(\frac{1}{2} + \gamma) & (\frac{1}{2} + \eta)(\frac{1}{2} - \gamma) \\ \frac{1}{4} - \frac{1}{2}\eta & (\frac{1}{2} + \eta)(\frac{1}{2} - \gamma) & (\frac{1}{2} + \eta)(\frac{1}{2} + \gamma) \end{bmatrix},$$

which is illustrated in Figure 2(b). We do not assume γ and η to be small, i.e., the channel does not have to be very noisy in this example.

There are two modes that information can be transmitted through this channel, corresponding to communicating through the two sub-channels described above. That is, to modulate the message in the input symbols 1 and $0 = \{2, 3\}$ of the BSC ($\frac{1}{2} - \eta$); or to modulate the message in the input symbols 2 and 3 of the BSC ($\frac{1}{2} - \gamma$).

Now, to apply our approach, we fix the empirical distribution P_X as $[\frac{1}{2} \ \frac{1}{4} \ \frac{1}{4}]^T$, and the corresponding output distribution P_Y is $[\frac{1}{2} \ \frac{1}{4} \ \frac{1}{4}]^T$. Then, the DTM is

$$B = \begin{bmatrix} \frac{1}{2} + \eta & \frac{1}{2\sqrt{2}} - \frac{1}{\sqrt{2}}\eta & \frac{1}{2\sqrt{2}} - \frac{1}{\sqrt{2}}\eta \\ \frac{1}{2\sqrt{2}} - \frac{1}{\sqrt{2}}\eta & (\frac{1}{2} + \eta)(\frac{1}{2} + \gamma) & (\frac{1}{2} + \eta)(\frac{1}{2} - \gamma) \\ \frac{1}{2\sqrt{2}} - \frac{1}{\sqrt{2}}\eta & (\frac{1}{2} + \eta)(\frac{1}{2} - \gamma) & (\frac{1}{2} + \eta)(\frac{1}{2} + \gamma) \end{bmatrix}.$$

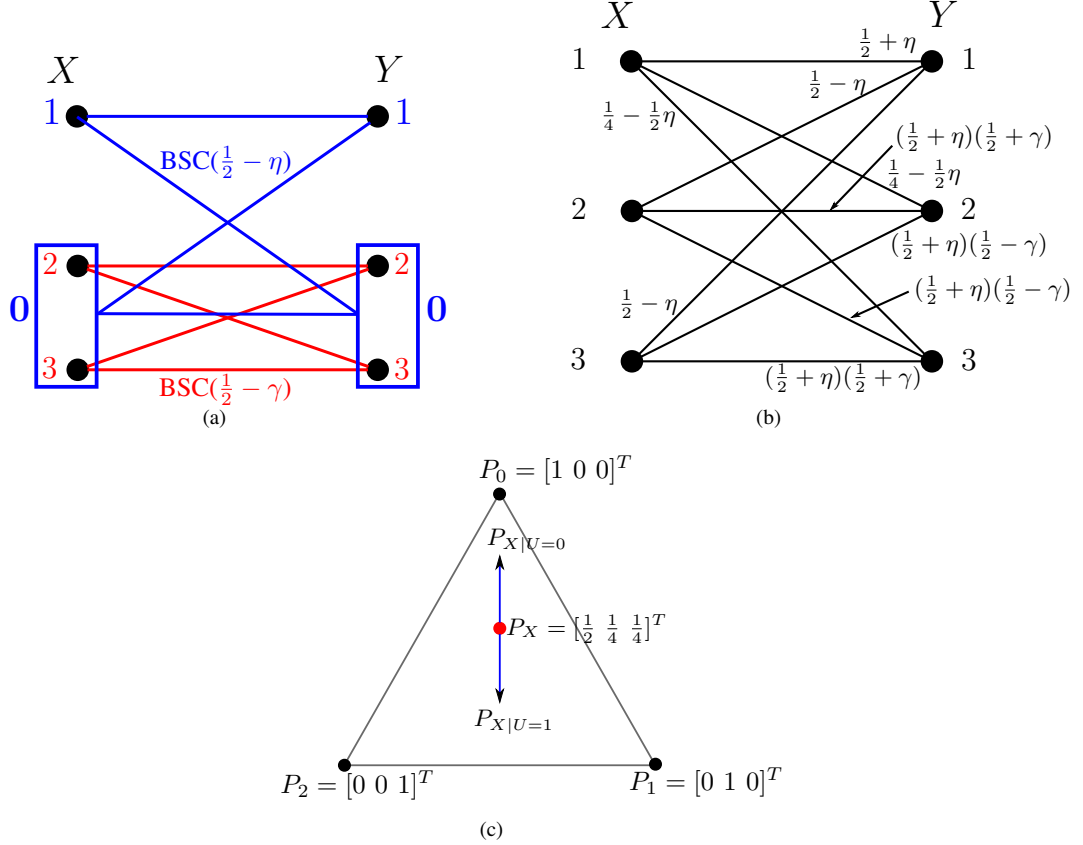


Fig. 2. (a) The ternary point-to-point channel that is composed of two binary symmetric channels. (b) The channel transition probability of this ternary channel. (c) The optimal perturbation direction for the ternary channel to convey information to the receiver end. Here, the triangle represents all valid input distributions, and the vertices are the deterministic input distributions of the three input symbols.

For this DTM, the singular values are 1, 2η , and $(1 + 2\eta)\gamma$, with the corresponding right singular vectors $[\frac{1}{\sqrt{2}} \ \frac{1}{2} \ \frac{1}{2}]^T$, $[\frac{1}{\sqrt{2}} \ \frac{-1}{2} \ \frac{-1}{2}]^T$, and $[0 \ \frac{1}{\sqrt{2}} \ \frac{-1}{\sqrt{2}}]^T$. Translating back to un-weighted perturbations, these corresponds to vectors $[\frac{1}{2}, \frac{1}{4}, \frac{1}{4}]^T$, $[\frac{1}{2}, -\frac{1}{4}, -\frac{1}{4}]^T$, and $[0, \frac{1}{4}, -\frac{1}{4}]^T$.

Note here if we perturb P_X along the first vector in any amount, it would result in an invalid distribution. The second and third perturbation vectors, correspond to the two transmission modes described above. For example, if we perturb along the second vector, we would have $P_{X|U=0} = [\frac{1}{2} + \frac{1}{2}\epsilon \ \frac{1}{4} - \frac{1}{4}\epsilon \ \frac{1}{4} - \frac{1}{4}\epsilon]^T$ and $P_{X|U=1} = [\frac{1}{2} - \frac{1}{2}\epsilon \ \frac{1}{4} + \frac{1}{4}\epsilon \ \frac{1}{4} + \frac{1}{4}\epsilon]^T$. This corresponds to increasing or decreasing the fraction of symbol 1 transmitted, according to the value of U .

The efficiency of these two modes depends on the two corresponding singular values. Here, the comparison is more in favor of the first mode, since given $P_X = [\frac{1}{2}, \frac{1}{4}, \frac{1}{4}]^T$, we can transmit symbol 2 or 3 only half of the time.

The point of this example is that for general problems, where we cannot identify naturally separable transmission modes by inspection, the SVD structure of the DTM matrix can always help us to do that like in this simple example.

B. The Single-Letterization

The most important feature of the linear information coupling problem (9) is that the single-letterization is simple. To illustrate the idea, we first consider a 2-letter version of the point-to-point channel:

$$\begin{aligned} & \max_{U \rightarrow X^2 \rightarrow Y^2} \frac{1}{2} I(U; Y^2), \\ & \text{subject to: } \frac{1}{2} I(U; X^2) \leq \frac{1}{2} \epsilon^2, \\ & \frac{1}{2} \|P_{X^2|U=u} - P_{X^2}\|^2 = O(\epsilon^2), \quad \forall u, \end{aligned} \tag{28}$$

Let P_X , P_Y , W , and B be the input and output distributions, channel matrix, and the DTM, respectively, for the single letter version of the problem. Then, the 2-letter problem has $P_X^{(2)} = P_X \otimes P_X$, $P_Y^{(2)} = P_Y \otimes P_Y$, and $W^{(2)} = W \otimes W$, where \otimes

denotes the Kronecker product. As a result, the new DTM is $B^{(2)} = B \otimes B$. Thus, the optimization in (28) has exactly the same form as in (13), where the only difference is that we need to find the SVD of $B^{(2)}$ instead of B . For that, we have the following lemma, the proof of which is omitted.

Lemma 2. *Let \underline{v}_i and \underline{v}_j denote two right (or left) singular vectors of B with singular values σ_i and σ_j . Then, $\underline{v}_i \otimes \underline{v}_j$ is a right (or left) singular vector of $B^{(2)}$ and the corresponding singular value is $\sigma_i \cdot \sigma_j$.*

Recall that the largest singular value of B is $\mu_0 = 1$, with the right singular vector $\underline{v}_0 = [\sqrt{P_X}, x \in \mathcal{X}]^T$, which corresponds to the direction orthogonal to the distribution simplex. This implies that the largest singular value of $B^{(2)}$ is also 1, corresponding to the singular vector $\underline{v}_0 \otimes \underline{v}_0$, which is again orthogonal to all valid choices of the weighted perturbation vectors.

The second largest singular value of $B^{(2)}$ is a tie between $\sigma_0 \cdot \sigma_1$ and $\sigma_1 \cdot \sigma_0$, with right singular vectors $\underline{v}_0 \otimes \underline{v}_1$ and $\underline{v}_1 \otimes \underline{v}_0$, where σ_1 is the second largest singular value of B , and \underline{v}_1 is the corresponding right singular vector. The optimal solution of (28) is thus the weighted perturbation vectors to be along the subspace spanned by these two vectors. This can be written as

$$P_{\underline{X}|U=u} = P_X \otimes P_X + \left[\sqrt{P_X \otimes P_X} \right] \cdot (\epsilon \underline{v}_0 \otimes \underline{v}_1 + \epsilon' \underline{v}_1 \otimes \underline{v}_0) \quad (29)$$

$$= \left(P_X + \epsilon' \left[\sqrt{P_X} \right] \underline{v}_1 \right) \otimes \left(P_X + \epsilon \left[\sqrt{P_X} \right] \underline{v}_1 \right) + O(\epsilon^2), \quad (30)$$

where (30) comes from noting that the vector $\underline{v}_0 = [\sqrt{P_X}, x \in \mathcal{X}]^T$, and adding the appropriate cross term for factorization. Here, we assume that ϵ and ϵ' are of the same order, which makes the cross term $O(\epsilon^2)$. This means that up to the first order approximation, the optimal choice of $P_{X^2|U=u}$, for any value of u , has a product form, i.e., the two transmitted symbols in X^2 are conditionally independent given U . With a simple time-sharing argument, we can see that it is optimal to set $\epsilon = \epsilon'$. This implies that picking $P_{X^2|U=u}$ to be i.i.d. over the two symbols achieves the optimal, with the approximation in (30).

Finally, by considering the n^{th} Kronecker product, we can generalize this procedure to the single-letterization of the n -letter problem (9).

Remark 5. This proof of showing the single-letter optimality is simple. All we have used is the fact that the singular vectors of $B^{(2)}$ corresponding to the second largest singular value has a special form, $\underline{v}_0 \otimes \underline{v}_1$ or $\underline{v}_1 \otimes \underline{v}_0$. We can visualize this as follows. The space of 2-letter joint distributions $P_{X^2|U=u}$ has $(|\mathcal{X}|^2 - 1)$ dimensions. Around the i.i.d. marginal distribution $P_X \otimes P_X$, there is a $2 \cdot (|\mathcal{X}| - 1)$ -dimensional subspace, such that the distributions in this subspace take the product form $Q_1 \otimes Q_2$, for some distributions Q_1 and Q_2 around P_X . These distributions can be written as perturbations from $P_X \otimes P_X$, with the weighted perturbations of the form $\underline{v}_0 \otimes \underline{v} + \underline{v}' \otimes \underline{v}_0$, for some \underline{v} and \underline{v}' orthogonal to \underline{v}_0 . The above argument simply verifies that the optimal solution to (28), which is the singular vectors of the $B^{(2)}$ matrix, has this form. We argue that this geometric view was not clear from the classical proofs of single-letterization. Moreover, it turns out that this procedure can be applied to more general problems. In section III and IV, we will demonstrate that in quite a few other multi-terminal problems, the similar structure can be proved and used for single-letterization.

We would like to emphasize that the advantage of our approach is that it does not require any constructive proving technique, such as constructing auxiliary random variables. For any given problem, one can follow essentially the same procedure to find out the SVD structure of the corresponding DTM. The result either gives a proof of the local optimality of the single-letter solutions or disproves it without any ambiguity.

C. Remarks On The Local Constraint (11)

Note that in our linear information coupling problem (1), we not only assume that the mutual information $\frac{1}{n}I(U; X^n)$ is small, but also restrict that the conditional distributions $P_{X^n|U=u}$ satisfy the local constraint $\frac{1}{n}\|P_{X^n|U=u} - P_{X^n}\|^2 = O(\epsilon^2)$, for all u . With the local constraint (11) on $P_{X^n|U=u}$, we can then guarantee the validity of the local approximation of K-L divergence in section II-A. Therefore, the local constraint (11) is indeed critical in order to obtain the linearized geometric structure.

Importantly, the local constraint (11) has to be specified independently from the constraint (10), because assuming $\frac{1}{n}I(U; X^n)$ to be small does not necessarily imply the local constraint on all the conditional distributions. It is possible that the joint distribution $P_{X^n U}$ satisfies $\frac{1}{n}I(U; X^n) \leq \frac{1}{2}\epsilon^2$, but the conditional distributions $P_{X^n|U=u}$ are far from P_{X^n} for some u 's, with the corresponding $P_U(u)$'s very small. Therefore, optimizing the mutual information $\frac{1}{n}I(U; Y^n)$ with only the constraint $\frac{1}{n}I(U; X^n) \leq \frac{1}{2}\epsilon^2$ can be a different problem from our linear information coupling problem.

In fact, Ahlswede and Gács in [15], and a recent paper by Nair *et al.* [16] considered the following quantity

$$s(X^n, Y^n) = \lim_{I(U; X^n) \rightarrow 0} \sup_{U \rightarrow X^n \rightarrow Y^n} \frac{I(U; Y^n)}{I(U; X^n)}, \quad (31)$$

where they established two important statements:

- (i) For i.i.d. $P_{X^n Y^n} = P_{X^n} P_{Y^n}$, the $s(X^n, Y^n)$ can be tensorized (single-letterized), i.e., $s(X^n, Y^n) = s(X, Y)$.
- (ii) In general, $s(X^n, Y^n)$ can be strictly larger than the σ_1^2 , where σ_1 is the second largest singular value of the divergence transition matrix B that we developed in section II-A.

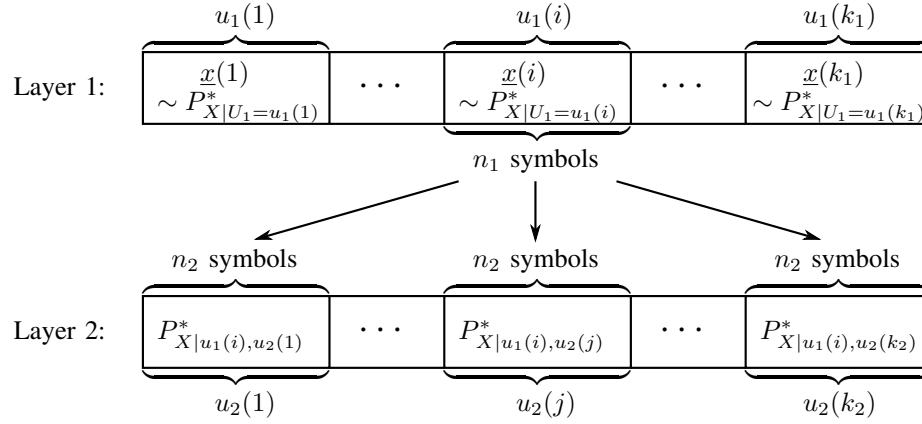


Fig. 3. The empirical distribution of different sub-blocks in each layer after encoding.

The statement (i) is an important property of $s(X^n, Y^n)$, because it addresses the single-letterization of the multi-letter problem in information theory, which reduces a computationally impossible problem to a computable one. On the other hand, the σ_1^2 we considered in our local geometry can also be tensorized by a linear algebra approach as we showed in section II-B. So, both $s(X^n, Y^n)$ and σ_1^2 have the tensorization property in this case of point-to-point communications.

Moreover, the statement (ii) implies that, without the local constraint, the optimal achievable information rate $\frac{1}{n}I(U; Y^n)$, subject to $\frac{1}{n}I(U; X^n) \leq \frac{1}{2}\epsilon^2$, is $s(X^n, Y^n) \cdot \frac{1}{2}\epsilon^2$. This is strictly better than the case with the local constraint, where the optimal achievable information rate is $\sigma_1^2 \cdot \frac{1}{2}\epsilon^2$. In that sense, $s(X^n, Y^n)$ is a strictly more meaningful quantity for this problem.

However, we would like to point out that it is still worth considering the quantity σ_1^2 . The value of the development we have shown so far in this paper does not lie in the tensorization result, but rather in the geometric method we used to arrive at this result. As we have stated in several different ways, the local assumptions fundamentally simplifies the problems involving tradeoff between multiple mutual information, which is the core of many problems seeking to find the multi-terminal capacity-regions. By taking this simplification, we focus on finding the local optimal solutions to the problem. In some sense, we have thus given up the hope of finding the globally optimal solution, and hence the hope of finding in general the capacity regions in the classical formulations. In return, the geometric insights from this approach does offer valuable guidance to code designs; and more importantly, it turns out that this simplification allows us to generalize our technique to the studies of network problems, in a conceptually straight forward way, which will be demonstrated in Section III. In contrast, the technique used in the non-local version of the problem, such as that used in proving the tensorization of $s(X^n, Y^n)$, is intrinsically based on the idea used in the study of degraded broadcast channels, and is difficult to generalize beyond a handful of canonical examples.

Before moving to the more interesting multi-terminal problems, we discuss in the rest two subsections that how the linear information coupling problems can be connected to the capacity problems, and also the relation between the linear information coupling problems and the Rényi maximal correlation. Readers, who are only interested in the application of our local approach to the multi-terminal problems, can directly turn to the section III and IV.

D. Capacity Achieving Layered Codes

In this subsection, we discuss one operational meaning of the linear information coupling problem, and try to connect to that of the conventional capacity problem for the point-to-point channels. To do that, we construct a channel code as superposition of many layers of codes, each layer constructed from the solution of a specific linear coupling problem. This construction is hardly useful in any practical situation, but rather serves as a conceptual tool to connect the two problems.

Let us start from the one-layer problem of this coding scheme. For a point-to-point channel with a transmitter X and a receiver Y , the goal of the one-layer problem is to efficiently transmit information through the Markov relation $U_1 \rightarrow X \rightarrow Y$, subject to the constraint $I(U_1; X) \leq \frac{1}{2}\epsilon^2$, and the local constraint $\|P_{X|U_1=u_1} - P_X\|^2 = O(\epsilon^2)$. From the analyses of the linear information coupling problem, we know how to find the optimal $P_{X|U_1=u_1}^*$ and $P_{U_1}^*$ to achieve the solution

$$r_1^* = \max_{\substack{U_1 \rightarrow X \rightarrow Y: I(U_1; X) \leq \frac{1}{2}\epsilon^2, \\ \|P_{X|U_1=u_1} - P_X\|^2 = O(\epsilon^2), \forall u_1}} I(U_1; Y) \quad (32)$$

Now, we propose the following coding scheme to explain the operational meaning of this solution. Suppose that there is a block³ of $n_1 \cdot k_1$ i.i.d. P_X distributed input symbols $\underline{x}(1), \dots, \underline{x}(k_1)$ generated at the transmitter, where $\underline{x}(i) \in \mathcal{X}^{n_1}$ represents a

³In this paper, all the “block length” and “number of sub-blocks” are assumed to be large.

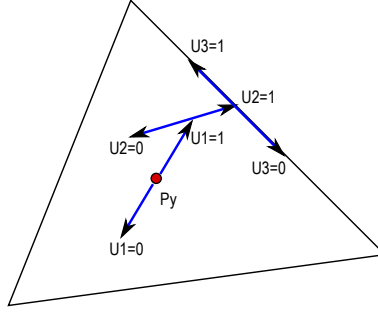


Fig. 4. A layered approach for the coding problem.

sub-block of n_1 input symbols $x_1(i), \dots, x_{n_1}(i)$, for $1 \leq i \leq k_1$. Then, we “encode” a binary codeword $u_1(1), \dots, u_1(k_1)$, with empirical distribution $P_{U_1}^*$, into this input symbol block by altering some of the symbols, such that the empirical distribution of each sub-block $\underline{x}(i)$ changes to $P_{X|U_1=u_1(i)}^*$. Note that the empirical distribution of the entire symbol block remains approximately the same as P_X^* . The receiver decodes this codeword according to different empirical output distributions of the k_1 sub-blocks. From (32), there exists binary block codes $u_1(1), \dots, u_1(k_1)$ with rate $R_1^* = n_1 \cdot r_1^*$ bits/ U_1 symbol, which can be reliably transmitted and decoded by using the above coding scheme. The empirical distributions of different blocks of input symbols, after this encoding procedure, are illustrated in Figure 3.

Now, we can add another layer to the one-layer problem. Theoretically, this is to consider a new set of linear information coupling problems

$$r_2^*(u_1) = \max_{\substack{(U_1, U_2) \rightarrow X \rightarrow Y: \\ \|P_{X|U_1=u_1, U_2=u_2} - P_{X|U_1=u_1}^*\|^2 = O(\epsilon^2), \forall u_2}} I(U_2; Y|U_1 = u_1), \quad (33)$$

where the conditional distribution of X given $U_1 = u_1$ is specified as $P_{X|U_1=u_1}^*$. We can solve (33) with the same procedure as (32), and find the optimal solutions $P_{X|U_1=u_1, U_2=u_2}^*$ and $P_{U_2|U_1=u_1}^*$.

Then, we can encode this one more layer of codewords to the original layer with a similar coding scheme. To do this, we further divide each sub-block $\underline{x}(i)$ into k_2 small sub-blocks, and each of the small sub-block has n_2 symbols, where $n_2 \cdot k_2 = n_1$. Then, for a binary code $u_2(1), \dots, u_2(k_2)$ with rate $R_2^*(u_1(i)) = n_2 \cdot r_2^*(u_1(i))$ bits/ U_2 symbol, where the distribution of the bits in the codewords is $P_{U_2|U_1=u_1(i)}^*$, we encode the codewords into small sub-blocks of $\underline{x}(i)$ by exactly the same coding scheme as the one-layer problem. The transmission rate of this coding scheme over the entire input symbol block $\underline{x}(1), \dots, \underline{x}(k_1)$ is then

$$\sum_{u_1} r_2^*(u_1) P_{U_1}^*(u_1) = I(U_2; Y|U_1) \quad \text{bits/transmission.}$$

After this, the empirical distribution of the j -th small sub-block of $\underline{x}(i)$ changes to $P_{X|U_1=u_1(i), U_2=u_2(j)}^*$, which is illustrated in Figure 3. On the other hand, the empirical distribution of the entire $\underline{x}(i)$ remains approximately the same as $P_{X|U_1=u_1(i)}^*$. Thus, the decoding of the codewords $u_1(1), \dots, u_1(k_1)$ of the first layer is not effected by adding the second layer, and can be proceeded as in the one-layer problem. The codewords of the second layer are then decoded after the first layer is decoded.

We can keep adding layers by recursively solving new linear information coupling problems, and sequentially applying the above layered coding scheme. Assuming that there is a sequence of messages U_1, U_2, \dots, U_K that we want to encode. First, we can find a perturbation of the P_X distribution according to the value of U_1 by solving the corresponding linear information coupling problem. Then, by solving the new set of information coupling problems conditioned on each value of $U_1 = u_1$, we can find further perturbations of that according to the value of U_2 , and so on. The corresponding perturbations in the output distribution space is illustrated in Figure 4.

Note that for each layer, say, layer k , while the channel matrix W remains the same, as we perturb only a sub-block of the symbols, the operating point is the empirical distribution of the sub-block $P_{X|U_1^{k-1}=u_1^{k-1}}$, which differs from the original P_X . Thus the resulting B matrix is also different. By this construction, we demonstrate that a channel code can be constructed through a sequence of layers, and thus can be viewed as an “integral” of a sequence of local perturbation problems. There are however several important differences between the two problems.

First, the most obvious issue is that since we divide the sub-blocks further with each layer of information, it appears that the sub-blocks gets very short as the number of layers increases. In fact, we can group all the sub-blocks with the same empirical distribution together before further division. For example, all the sub-blocks in Figure 4 with length n_1 with the corresponding $u_1(i) = 0$ can be grouped together before further dividing. In more general cases, some sub-blocks from different branches

might end up having the same or approximately the same empirical distributions, and thus grouped together. Thus, the total number of sub-blocks at each layer is limited by the granularity of empirical distributions we choose to group sub-blocks, and does not have to increase exponentially with the number of layers.

The second issue, as shown in Figure 4, the valid choices of distributions on the channel output must be in a convex region. For a given channel matrix W , whose column vectors are the conditional distributions of the output Y , conditioned on different values of the channel input $X = x$, the output distributions must belong to the convex region specified by these column vectors. As we add more layers, at some point the boundary of this convex region is reached. From which point, further layering is restricted to be along the hypersurface of this convex region. Conceptually, there is not much difference, since moving the output distributions on the hypersurface corresponds to not use a subset of the input alphabet. Hence, a local problem can in principle be written out with a reduced input alphabet. This can indeed be done in some special cases [7]. However, for general problems, especially multi-letter problems, specifying this high dimensional convex region and all its boundary constraints seems to be a reason that forbids general analytical solutions.

Finally, the most significant difference between the two problems is that although a channel code is constructed as superposition of many layers of codes, optimizing the coupling efficiency at each individual layer, i.e., using the solution we specified in (27), for each layer, does not necessarily yield the optimality of the overall code. This is because at each layer we not only convey the corresponding layer of information through the channel, but also the resulting empirical distributions of sub-blocks become the operating points for the future layers. Thus, the construction of overall channel code can be viewed as a dynamic programming, where each layer not only needs to carry as much information as possible, but also needs to set up favorable operating points for the future layers. Our solution based on SVD analysis can thus be viewed as a greedy solution to the channel coding problem.

For some special cases, especially if the channel considered is very noisy, we can indeed use the above approach to design a capacity achieving channel code. The following is one of such examples.

Example 2. We continue to use the example 1, but make the channel very noisy by setting both the parameters γ and η to be close to 0. We assume γ/η remains constant, and consider only the case that $\gamma < \eta$. We apply the layered coding scheme to construct a capacity achieving code.

First, ignoring the higher order terms, the channel capacity of the ternary channel in Figure 2(b) is $2\eta^2 + (\frac{1}{2} + \eta)\gamma^2$, with the optimal input distribution $P_X = [\frac{1}{2} \ \frac{1}{4} \ \frac{1}{4}]^T$. From example 1, we know that when $\gamma > \eta$, the optimal perturbation vector is $[\frac{1}{2} \ \frac{-1}{4} \ \frac{-1}{4}]^T$, and the corresponding conditional distributions are $P_{X|U_1=0} = [\frac{1}{2} + \frac{1}{2}\epsilon \ \frac{1}{4} - \frac{1}{4}\epsilon \ \frac{1}{4} - \frac{1}{4}\epsilon]^T$ and $P_{X|U_1=1} = [\frac{1}{2} - \frac{1}{2}\epsilon \ \frac{1}{4} + \frac{1}{4}\epsilon \ \frac{1}{4} + \frac{1}{4}\epsilon]^T$. To apply the layered coding scheme, we keep increasing the perturbation vector until the boundary is reached, i.e., increasing⁴ ϵ to 1. Then, the conditional distribution $P_{X|U_1=0}$ reaches the vertex $[1 \ 0 \ 0]^T$, and $P_{X|U_1=1}$ reaches the boundary at $[0 \ \frac{1}{2} \ \frac{1}{2}]^T$. This is shown in Figure 5. The achievable information rate by the first layer of perturbation is $I(U_1; Y) = \frac{1}{2}\epsilon^2(2\eta)^2 = 2\eta^2$.

To achieve this rate, we divide the n bit codeword into k_1 sub-blocks, each with n_1 bits, and use a binary code of length k_1 , with rate $R_1 = (2\eta^2) \cdot n_1$. We choose n_1 appropriately to make sure $R_1 < 1$. The total number of information bits encoded is $k_1 R_1 = n \cdot 2\eta^2$. The k_1 coded bits are assigned to each sub-block. The sub-blocks corresponding to a coded bit of 0 are filled with channel symbol '1's. The rest of sub-blocks should be filled with half '2's and half '3's. We group these sub-blocks together, of total length $n/2$, for the second layer of information. To do that, we further divide these $n/2$ symbols into k_2 sub-blocks, each with n_2 symbols.

We perturb the conditional distribution $P_{X|U_1=1} = [0 \ \frac{1}{2} \ \frac{1}{2}]^T$. Note that this distribution has already reached the boundary of the simplex, and we cannot further reduce the probability of '0'. Thus, the perturbation is along this boundary. This corresponds to a linear information coupling problem with reduced input alphabet of just $\{2, 3\}$. Therefore, the DTM of this problem has reduced dimension, and can be explicitly computed as

$$B_2 = \begin{bmatrix} \sqrt{\frac{1}{4} - \frac{1}{2}\eta} & \sqrt{\frac{1}{4} - \frac{1}{2}\eta} \\ \sqrt{\frac{1}{2} + \eta} \left(\frac{1}{2} + \gamma\right) & \sqrt{\frac{1}{2} + \eta} \left(\frac{1}{2} - \gamma\right) \\ \sqrt{\frac{1}{2} + \eta} \left(\frac{1}{2} - \gamma\right) & \sqrt{\frac{1}{2} + \eta} \left(\frac{1}{2} + \gamma\right) \end{bmatrix}.$$

The second largest singular value of this DTM is $\sigma_1 = \sqrt{2 + 4\eta} \cdot \gamma$, and the corresponding singular vector is $\underline{v}_1 = [0 \ \frac{1}{\sqrt{2}} \ \frac{-1}{\sqrt{2}}]^T$. Observe that this new singular value is smaller than that for the first layer, indicating less efficient coupling of information. The optimal perturbation vector is $[0 \ \frac{1}{2} \ \frac{-1}{2}]^T$, and the conditional distributions are $P_{X|U_1=1, U_2=0} = [0 \ \frac{1}{2} + \frac{1}{2}\epsilon \ \frac{1}{2} - \frac{1}{2}\epsilon]^T$ and $P_{X|U_1=1, U_2=1} = [0 \ \frac{1}{2} - \frac{1}{2}\epsilon \ \frac{1}{2} + \frac{1}{2}\epsilon]^T$. We choose $\epsilon = 1$, so the perturbed distributions reach the two vertices $[0 \ 1 \ 0]^T$ and $[0 \ 0 \ 1]^T$, as shown in Figure 5.

⁴Since we assume both η and γ are small, the local approximation of all divergence and mutual information of interests remains valid even if ϵ is not small. This is why we can increase ϵ here from a small number to 1 without violating the local approximation.

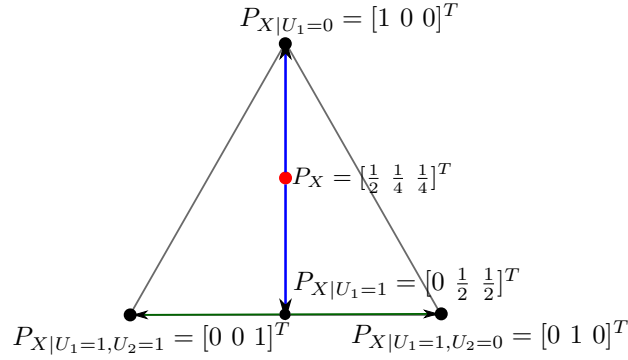


Fig. 5. In the first layer, the input distribution P_X is perturbed to $P_{X|U_1=0}$ and $P_{X|U_1=1}$, where $P_{X|U_1=0}$ reaches one of the vertices, and $P_{X|U_1=1}$ reaches the boundary. In the second layer, the distribution $P_{X|U_1=1}$ is further perturbed to $P_{X|U_1=1, U_2=0}$ and $P_{X|U_1=1, U_2=1}$, where the rest two vertices are reached.

The achievable information rate by the second layer of perturbation is

$$I(U_2; Y|U_1) = I(U_2; Y|U_1 = 1) \cdot P(U_1 = 1) = \frac{1}{2} \epsilon^2 (\sqrt{2 + 4\eta} \cdot \gamma)^2 \cdot \frac{1}{2} = \left(\frac{1}{2} + \eta\right) \gamma^2.$$

In terms of the code construction, this second layer of information is conveyed by using a binary code of length k_2 , with rate $R_2 = 2 \cdot n_2 \cdot \left(\frac{1}{2} + \eta\right) \gamma^2$. The total number of information bits carried is thus $k_2 \cdot R_2 = n \cdot \left(\frac{1}{2} + \eta\right) \gamma^2$. These k_2 coded bits are assigned to the corresponding sub-blocks. Those assigned with a 0 are filled with transmitted symbol '2's, and the others with '3's.

After these two layers of perturbations, all the conditional distributions reach the vertices, and the total achievable information rate is $2\eta^2 + \left(\frac{1}{2} + \eta\right) \gamma^2$, which achieves the channel capacity of this ternary channel.

Note that resulting code repeats symbol '1' for n_1 times, symbols '2' and '3' for n_2 times. Such repetition is indeed expected for codes that achieve the capacity for very noisy channels.

E. The relation to Rényi maximal correlation

In this subsection, we show that the second largest singular value of the DTM is precisely the same as the Rényi maximal correlation between random variables X and Y , where the marginal distributions P_X and P_Y are the given input and output distributions in the linear information coupling problem (13), and the transition probability kernel $P_{Y|X}$ is the channel W . Let us begin with the following definition.

Definition 1. [12] The Rényi maximal correlation $\rho_m(X, Y)$ between two random variables X and Y is defined by

$$\rho_m(X, Y) = \sup E[f(X)g(Y)], \quad (34)$$

where the supremum is over all Borel-measurable functions f and g such that

$$\begin{aligned} E[f(X)] &= E[g(Y)] = 0, \\ E[f^2(X)] &= E[g^2(Y)] = 1. \end{aligned} \quad (35)$$

The Rényi maximal correlation is a measure of dependence of random variables that is stronger and more general than the correlation coefficient, since it allows arbitrary zero-mean, unit-variance functions of X and Y . The Rényi maximal correlation is first introduced by Hirschfeld [9] and Gebelein [10] for discrete random variables and absolutely continuous random variables. Rényi [11], [12] compared the Rényi maximal correlation to other measures of dependence, and provided sufficient conditions for which the supremum of (34) is achieved. In particular, for discrete random variables X and Y , the sufficient conditions are met, and Rényi maximal correlation can be attained. Moreover, Rényi showed that if the function pair (\hat{f}, \hat{g}) achieves (34), then

$$\begin{aligned} E[\hat{g}(Y)|X] &= \rho_m(X, Y)\hat{f}(X), \\ E[\hat{f}(X)|Y] &= \rho_m(X, Y)\hat{g}(Y). \end{aligned} \quad (36)$$

Now to see the connection between DTM and the above results, we write \mathcal{F}_X and \mathcal{G}_Y as the spaces of real-valued functions on \mathcal{X} and \mathcal{Y} , resp; and consider the conditional expectation operator $E[\cdot|X] : \mathcal{G}_Y \mapsto \mathcal{F}_X$ as a map that takes a function of y to a function of x . We use $\langle \cdot, \cdot \rangle_{P_X}$ and $\langle \cdot, \cdot \rangle_{P_Y}$ as inner products on \mathcal{F}_X and \mathcal{G}_Y . This is convenient, as for example (35) can

be written as

$$\begin{aligned} E[f(X)] &= \langle f, \mathbf{1}_X \rangle_{P_X} = 0, \\ E[g(Y)] &= \langle g, \mathbf{1}_Y \rangle_{P_Y} = 0, \\ E[f^2(X)] &= \langle f, f \rangle_{P_X} = \|f\|^2 = 1, \\ E[g^2(Y)] &= \langle g, g \rangle_{P_Y} = \|g\|^2 = 1, \end{aligned}$$

which are simple orthogonality and norm constraints. In the above, we used the notation $\mathbf{1}_X$ and $\mathbf{1}_Y$ as the constant 1 functions.

We also define functions

$$\begin{cases} \phi_{x'}(\cdot) = \sqrt{P_X(\cdot)}^{-1} \cdot \delta_{x'}(\cdot), & x' \in \mathcal{X} \\ \varphi_{y'}(\cdot) = \sqrt{P_Y(\cdot)}^{-1} \cdot \delta_{y'}(\cdot), & y' \in \mathcal{Y} \end{cases}, \quad (37)$$

where

$$\delta_{x'}(x) = \begin{cases} 1, & \text{if } x = x' \\ 0, & \text{otherwise} \end{cases}, \quad \delta_{y'}(y) = \begin{cases} 1, & \text{if } y = y' \\ 0, & \text{otherwise} \end{cases},$$

It can be verified that these two groups of functions in (37) all have unit norm, and are orthogonal within each group. Thus, they form orthonormal bases of \mathcal{F}_X and \mathcal{G}_Y respectively. We now can write the conditional expectation operator $E[\cdot|X]$ in matrix form, with respect to these bases. To do that, consider the (x', y') entry

$$\begin{aligned} & \langle \phi_{x'}, E[\varphi_{y'}|X = x] \rangle_{P_X} \\ &= \sum_{x \in \mathcal{X}} P_X(x) \cdot \left(\sqrt{P_X(x)}^{-1} \delta_{x'}(x) \right) \cdot E[\varphi_{y'}|X = x] \\ &= \sqrt{P_X(x')} \cdot \left(\sum_{y \in \mathcal{Y}} \sqrt{P_Y(y)}^{-1} \delta_{y'}(y) P_{Y|X}(y|x') \right) \\ &= \sqrt{P_Y(y')}^{-1} P_{Y|X}(y'|x') \sqrt{P_X(x')}. \end{aligned}$$

Therefore, this matrix is precise the DTM as we defined. Repeating the same derivation for the operator $E[\cdot|Y]$ reveals that the two operators $E[\cdot|X]$ and $E[\cdot|Y]$ are indeed conjugates of each other. Furthermore, there is a one-to-one correspondence between the singular vectors of the DTM and the singular functions of the conditioned expectation operator. In particular, note that the all-1 function $\mathbf{1}_X$ and $\mathbf{1}_Y$ has the nice properties $E[\mathbf{1}_Y|X] = \mathbf{1}$, and $E[\mathbf{1}_X|Y] = \mathbf{1}_Y$. Thus, $\mathbf{1}_X$ and $\mathbf{1}_Y$ are a pair of input and output singular functions of the conditional expectation operator, with singular vector 1. This corresponds to the first singular vector $\left[\sqrt{P_X(x)}, x \in \mathcal{X} \right]^T$ of the DTM. In addition, note that the zero-mean constraint (35) on functions in \mathcal{F}_X is equivalent to the orthogonality to $\mathbf{1}_X$. Therefore, the rest singular functions of the conditioned expectation operator satisfy (35), and have a one-to-one correspondence to the singular vectors of the DTM other than the first one.

From (36), we know that the pair of function (\hat{f}, \hat{g}) that achieves the maximal correlation must be a pair of input/output singular vectors of the conditional expectation operator. The fact that such correlation $|\rho_m(X, Y)|$ is no larger than 1 quantifies the contraction behavior of the operators, and is a manifestation of the data processing inequality. We summarize in the following proposition.

Proposition 1. *The second largest singular value of the DTM is the Rényi maximal correlation $\rho_m(X, Y)$. Moreover, the functions \hat{f} and \hat{g} maximizing (34) can be obtained from the left and right singular vectors of the DTM with the second largest singular value, corresponding to the orthonormal bases (37).*

The relation between (13) and the Rényi maximal correlation $\rho_m(X, Y)$ was also shown in [8] and [17] by different approaches. The value of this connection, to our purpose, is that it provides yet another view of the local approximation approach. More interestingly, if we recall that Rényi's original work on maximal correlation was to characterize the dependence between two random variables; now the spectrum analysis of the DTM, or the conditional expectation operator, provides us with a broader range of quantities that might be of interests. For example, now we can ask not only about the maximal correlation, but also "second" maximal correlation, which corresponds to the largest two singular values of the DTM. In the following sections, we will generalize the concept to multi-terminal cases, which potentially leads to concepts such as the maximal correlation between more than two random variables. As we will show, this generalization is indeed quite simple if we keep the local approximations.

III. THE GENERAL BROADCAST CHANNELS

In this section, we apply the local approximation approach to general broadcast channels, and study the corresponding linear information coupling problems. We first illustrate our technique by considering the 2-user broadcast channel, and then the extension to the K -user case is straight forward.

A 2-user general broadcast channel with input $X \in \mathcal{X}$, and outputs $Y_1 \in \mathcal{Y}_1$, $Y_2 \in \mathcal{Y}_2$, is specified by the memoryless channel matrices W_1 and W_2 . These channel matrices specify the conditional distributions of the output signals at two users, 1 and 2, as $W_i(y_i|x) = P_{Y_i|X}(y_i|x)$, for $i = 1, 2$. Let M_1 , M_2 , and M_0 be the two private messages and the common message, with rate R_1 , R_2 , and R_0 , respectively. Then, using Fano's inequality, the multi-letter capacity region of the general broadcast channel is the set of rate tuple (R_0, R_1, R_2) such that

$$\begin{cases} R_0 & \leq \frac{1}{n} \min\{I(U; \underline{Y}_1), I(U; \underline{Y}_2)\}, \\ R_1 & \leq \frac{1}{n} I(V_1; \underline{Y}_1), \\ R_2 & \leq \frac{1}{n} I(V_2; \underline{Y}_2), \end{cases} \quad (38)$$

for some mutually independent random variables U , V_1 , and V_2 , such that $(U, V_1, V_2) \rightarrow \underline{X} \rightarrow \underline{Y}_1$ and $(U, V_1, V_2) \rightarrow \underline{X} \rightarrow \underline{Y}_2$, are both Markov chains. The signal vectors here all have the same dimension n . In principle, one should just optimize this rate region by finding the optimal coding distributions. However, since n can potentially be arbitrarily large, finding the structure of these optimal input distributions is necessary.

Now, we want to apply the local approximation technique we developed in section II to this broadcast channel problem. As a natural generalization from the point-to-point channel case (9), the linear information coupling problem of this 2-user broadcast channel is the characterization of the rate region:

$$\begin{aligned} & \begin{cases} R_0 \leq \frac{1}{n} \min\{I(U; \underline{Y}_1), I(U; \underline{Y}_2)\} \\ R_1 \leq \frac{1}{n} I(V_1; \underline{Y}_1) \\ R_2 \leq \frac{1}{n} I(V_2; \underline{Y}_2) \end{cases} \\ \text{subject to: } & (U, V_1, V_2) \rightarrow \underline{X} \rightarrow (\underline{Y}_1, \underline{Y}_2), \\ & \frac{1}{n} I(U, V_1, V_2; \underline{X}) \leq \frac{1}{2} \epsilon^2, \\ & \frac{1}{n} \|P_{\underline{X}|(U, V_1, V_2)=(u, v_1, v_2)} - P_{\underline{X}}\|^2 = O(\epsilon^2), \\ & \forall (u, v_1, v_2) \in \mathcal{U} \times \mathcal{V}_1 \times \mathcal{V}_2, \end{aligned} \quad (39)$$

where U, V_1, V_2 are mutually independent random variables.

This rate region is the same as the capacity region (38) except for the local constraints. The operational meaning of these constraints are similar to that for the point-to-point case. That is, we consider modulating all the common and private messages entirely as a thin layer of information into the input symbol sequence \underline{X} .

The first simplifying observation is that the characterization of (39) involves the optimization over multiple rates R_0 , R_1 , and R_2 , with respect to different messages M_0 , M_1 , and M_2 . This can indeed be separated into three sub-problems. The idea here is that, while the conditional distribution $P_{\underline{X}|(U, V_1, V_2)=(u, v_1, v_2)}$ is perturbed from $P_{\underline{X}}$ by some vector J_{u, v_1, v_2} that is in general a joint function of U , V_1 , and V_2 , by the first order approximation, it is enough to only consider perturbation vectors that can be written as the linear combination of three vectors J_u , J_{v_1} , and J_{v_2} . This fact is shown in the following Lemma.

Lemma 3. *The rate region (39) is, up to the first order approximation, the same as the following rate region with the constraints separated for U , V_1 , and V_2 :*

$$\begin{aligned} & \begin{cases} R_0 \leq \frac{1}{n} \min\{I(U; \underline{Y}_1), I(U; \underline{Y}_2)\} \\ R_1 \leq \frac{1}{n} I(V_1; \underline{Y}_1) \\ R_2 \leq \frac{1}{n} I(V_2; \underline{Y}_2) \end{cases} \\ \text{subject to: } & (U, V_1, V_2) \rightarrow \underline{X} \rightarrow (\underline{Y}_1, \underline{Y}_2), \frac{1}{n} I(U; \underline{X}) \leq \frac{1}{2} \epsilon_0^2, \\ & \frac{1}{n} I(V_1; \underline{X}) \leq \frac{1}{2} \epsilon_1^2, \frac{1}{n} I(V_2; \underline{X}) \leq \frac{1}{2} \epsilon_2^2, \sum_{i=1}^3 \epsilon_i^2 = \epsilon^2 \\ & \frac{1}{n} \|P_{\underline{X}|(U, V_1, V_2)=(u, v_1, v_2)} - P_{\underline{X}}\|^2 = O(\epsilon^2), \\ & \forall (u, v_1, v_2) \in \mathcal{U} \times \mathcal{V}_1 \times \mathcal{V}_2, \end{aligned} \quad (40)$$

Proof: Appendix A. ■

Now for a tuple of $(\epsilon_0, \epsilon_1, \epsilon_2)$ with $\sum_{i=1}^3 \epsilon_i^2 = \epsilon^2$, the optimization problem (40) reduces to three sub-problems: for $i = 1, 2$,

the optimization problems for transmitting the private messages M_i

$$\begin{aligned} \max. \quad & \frac{1}{n} I(V_i; \underline{Y}_i) \\ \text{subject to:} \quad & V_i \rightarrow \underline{X} \rightarrow \underline{Y}_i, \frac{1}{n} I(V_i; \underline{X}) \leq \frac{1}{2} \epsilon_i^2, \\ & \frac{1}{n} \|P_{\underline{X}|V_i=v_i} - P_{\underline{X}}\|^2 = O(\epsilon_i^2), \forall v_i, \end{aligned} \quad (41)$$

and the optimization problem for the common message M_0

$$\begin{aligned} \max. \quad & \frac{1}{n} \min \{I(U; \underline{Y}_1), I(U; \underline{Y}_2)\} \\ \text{subject to:} \quad & U \rightarrow \underline{X} \rightarrow (\underline{Y}_1, \underline{Y}_2), \frac{1}{n} I(U; \underline{X}) \leq \frac{1}{2} \epsilon_0^2, \\ & \frac{1}{n} \|P_{\underline{X}|U=u} - P_{\underline{X}}\|^2 = O(\epsilon_0^2), \forall u. \end{aligned} \quad (42)$$

As in the point-to-point channel case, we assume that the input distribution of \underline{X} , as the operating point, is i.i.d. P_X . Hence, the output distributions of the two outputs Y_1 and Y_2 are also i.i.d. P_{Y_1} and P_{Y_2} . The conditional distributions is denoted as perturbations from the marginal distribution, which are written as $P_{\underline{X}|U=u} = P_X^{(n)} + \sqrt{n}\epsilon_0 \cdot J_u$ and $P_{\underline{X}|V_i=v_i} = P_X^{(n)} + \sqrt{n}\epsilon_i \cdot J_{v_i}$ for $i = 1, 2$.

Then, the optimization problems (41) for private messages are the same as the linear information coupling problem for the point-to-point channel (9). Thus, by defining the single-letter DTM's $B_i \triangleq \left[\sqrt{P_{Y_i}}^{-1} \right] W_i \left[\sqrt{P_X} \right]$ for $i = 1, 2$, we can solve (41) with the same procedure as (9), and the single-letter solutions are optimal.

The optimization problem (42) is, however, fundamentally different from the other two. Suppose that the weighted perturbation vector $\psi_u = \left[\sqrt{P_X^{(n)}}^{-1} \right] J_u$, the local version of the problem can be written as

$$\max_{\psi_u} \min \left\{ \sum_u P_U(u) \|B_1^{(n)} \psi_u\|^2, \sum_u P_U(u) \|B_2^{(n)} \psi_u\|^2 \right\}, \quad (43)$$

subject to

$$\sum_u P_U(u) \cdot \|\psi_u\|^2 = 1,$$

and also the constraints (21) and (22) that guarantee the validity of the weighted perturbation vector. Here, the $B_i^{(n)}$ is the n^{th} Kronecker product of the single-letter DTM B_i , for $i = 1, 2$.

Our goal here is to check whether there exists a single-letter optimal solution for the problem of transmitting the common message (43). Similar to the process of analyzing the point-to-point problem, this is carried out in several steps: 1) we need to check whether the optimal solution in (43), perturbation vectors ψ_u^* , leads to $P_{\underline{X}|U=u}$ that take product form; 2) we hope to find a time-sharing/convexity argument to show that the optimal choices of $P_{\underline{X}|U=u}$ are not only independent, but also identical from letter to letter; 3) we need to have control over the cardinality of U . In particular, we would hope that the cardinality of U does not change with n , and should not increase with K , the number of receivers of the broadcast channel.

Before answering these questions in a formal statement, we would first make some intuitive discussions, to point out the key differences between the broadcast channel and the point-to-point case.

The key difference between the optimization problem (43) and its counterpart for the point-to-point channel (19) is that we want to design a set of perturbation vectors, whose images through two separate linear maps, $B_1^{(n)}$ and $B_2^{(n)}$, are large at the same time. This involves the tradeoff between two linear systems, and is exactly the key issue in broadcasting common messages.

While generally the tradeoff between two linear systems can be a rather messy problem, the special structure of $B_1^{(n)}$ and $B_2^{(n)}$ turns out to be quite useful. Since both $i = 1, 2$, $B_i^{(n)}$ is the tensor product of the corresponding single-letter DTM's B_i , the singular vectors of $B_i^{(n)}$ also take the form of tensor products of the singular vectors of B_i . That is, if $\underline{v}_{i,0}, \underline{v}_{i,1}, \dots, \underline{v}_{i,M}$ are the singular vectors of B_i , with the corresponding singular values $\sigma_{i,0} \geq \sigma_{i,1} \geq \dots \geq \sigma_{i,M}$, then for any $j_1, j_2, \dots, j_n \in \{0, \dots, M\}$

$$\underline{v}_{i,j_1} \otimes \underline{v}_{i,j_2} \otimes \dots \otimes \underline{v}_{i,j_n} \quad (44)$$

is a singular vector for $B_i^{(n)}$, with the corresponding singular value $\sigma_{i,j_1} \cdot \sigma_{i,j_2} \cdot \dots \cdot \sigma_{i,j_n}$. For each $i \in \{1, 2\}$, the corresponding collection of singular vectors form an orthonormal basis on the space of joint distributions over X_1, \dots, X_n .

Moreover, B_1 and B_2 share the same largest singular value $\sigma_{i,0} = 1$ and the same corresponding singular vector $\underline{v}_{i,0} = [\sqrt{P_X(x)}, x \in \mathcal{X}]^T$. This means that both linear systems $B_1^{(n)}$ and $B_2^{(n)}$ output larger images for those singular vectors of the form (44) with smaller indices j_1, \dots, j_n . Note that the vector with $j_1 = j_2 = \dots = j_n = 0$ is an invalid choice of perturbation vector, thus a direction with large output images through both systems should have all but one of the indices equal to 0. Put it another way, if we pick a perturbation vector that has a non-zero image in the form of (44), with any choice of j_1, \dots, j_n , then replacing all but one indices by 0 would result in a larger image through both $B_1^{(n)}$ and $B_2^{(n)}$. Formalizing this argument, we can conclude that the optimizer of (43) must be ψ_u 's that are linear combinations of these singular vectors. This corresponds precisely to a resulting $P_{\underline{X}|U=u}$ in the product form, i.e., X_1, X_2, \dots, X_n are independent conditioned on U , just like in the point-to-point case.

The main difference between the broadcasting channel and the point-to-point channel comes with the choice of P_U . Recall previously, in (24), we used the fact that for any choice of the direction of ψ , there is a linear relation between the constraint on $\|\psi\|^2$ and the objective $\|B\psi\|^2$ to conclude that one can without loss of generality pick P_U to be the binary uniform distribution, and focus only on choosing a single direction of ψ that maximizes the ratio $\|B\psi\|^2/\|\psi\|^2$. In the broadcast channel, however, since our objective function is the minimum output image from multiple linear systems, the above argument no longer holds. In fact, in some cases, it can be beneficial to choose multiple ψ_u 's with different directions, and average over the output squared norms, as without the averaging, some of such choices might be eliminated by the $\min\{\cdot, \cdot\}$ operation. In fact, when we have $K > 2$ receivers, the objective function becomes the minimum among the outputs of K linear systems, and the number of ψ_u 's we need to achieve the optimum increases with K . This is summarized in the following Theorem and example.

Theorem 1. *Let B_i be the DTM of some DMC with respect to the same input distributions P_X , for $i = 1, 2, \dots, K$, let $\underline{v}_0 = [\sqrt{P_X(x)}, x \in \mathcal{X}]^T$ be the common singular vector of B_i with the largest singular value of 1, and $\underline{v}_0^{(n)} = \underline{v}_0 \otimes \underline{v}_0, \dots, \underline{v}_0$ be the n -th Kronecker product, then for the linear information coupling problem*

$$\lambda^{(n)} = \max \min_{1 \leq i \leq K} \left\{ \sum_u P_U(u) \cdot \|B_i^{(n)} \psi_u\|^2 \right\}, \quad (45)$$

where the maximization is taken over all $P_U(\cdot)$ and ψ_u such that

$$\begin{aligned} \sum_u P_U(u) \cdot \|\psi_u\|^2 &= 1 \\ \langle \psi_u, \underline{v}_0^{(n)} \rangle &= 0, \quad \forall u \end{aligned}$$

we have

- a) *There exists an optimal choice where ψ_u for all u take product form:*

$$\psi_u = \underline{v}^{(1)} \otimes \underline{v}^{(2)} \otimes \dots \otimes \underline{v}^{(n)}$$

where all but one of the $\underline{v}^{(i)}$'s are equal to \underline{v}_0 .

- b) $\lambda^{(n)} = \lambda^{(1)}$ with the cardinality of U no larger than K
c) *With the extra constraint that U is binary and the two corresponding ψ_u 's lie in the same direction, the problem becomes*

$$\lambda_B^{(n)} = \max_{\psi: \|\psi\|^2=1, \langle \psi, \underline{v}_0 \rangle=0} \min_{1 \leq i \leq K} \left\{ \|B_i^{(n)} \psi\|^2 \right\}$$

We have

$$\sup_n \lambda_B^{(n)} = \begin{cases} \lambda_B^{(1)} & \text{if } k = 2, \\ \lambda_B^{(k)} & \text{if } k > 2, \end{cases}$$

and for $k > 2$, there exists k -user broadcast channels such that

$$\lambda^{(k)} > \lambda^{(k-1)}.$$

In other words, with a constraint on the cardinality of U , single-letter solutions are not optimal in general. However, there always exists a K -letter optimal solution.

Proof: See Appendix B. ■

The following example illustrates that when there are more than 2 receivers, i.i.d. distributions simply do not have enough degrees of freedom to be optimal in the tradeoff of the K linear systems. Therefore, one has to design multi-letter product distributions to achieve the optimal. The following example, constructed with the geometric method, illustrates the key ideas.

Example 3 (The windmill channel). We consider a 3-user broadcast channel as shown in Figure 6(a). The input alphabet \mathcal{X} is ternary, so that the perturbation vectors have 2 dimensions and can be easily visualized. Suppose that P_X is fixed as $[\frac{1}{3} \ \frac{1}{3} \ \frac{1}{3}]^T$,

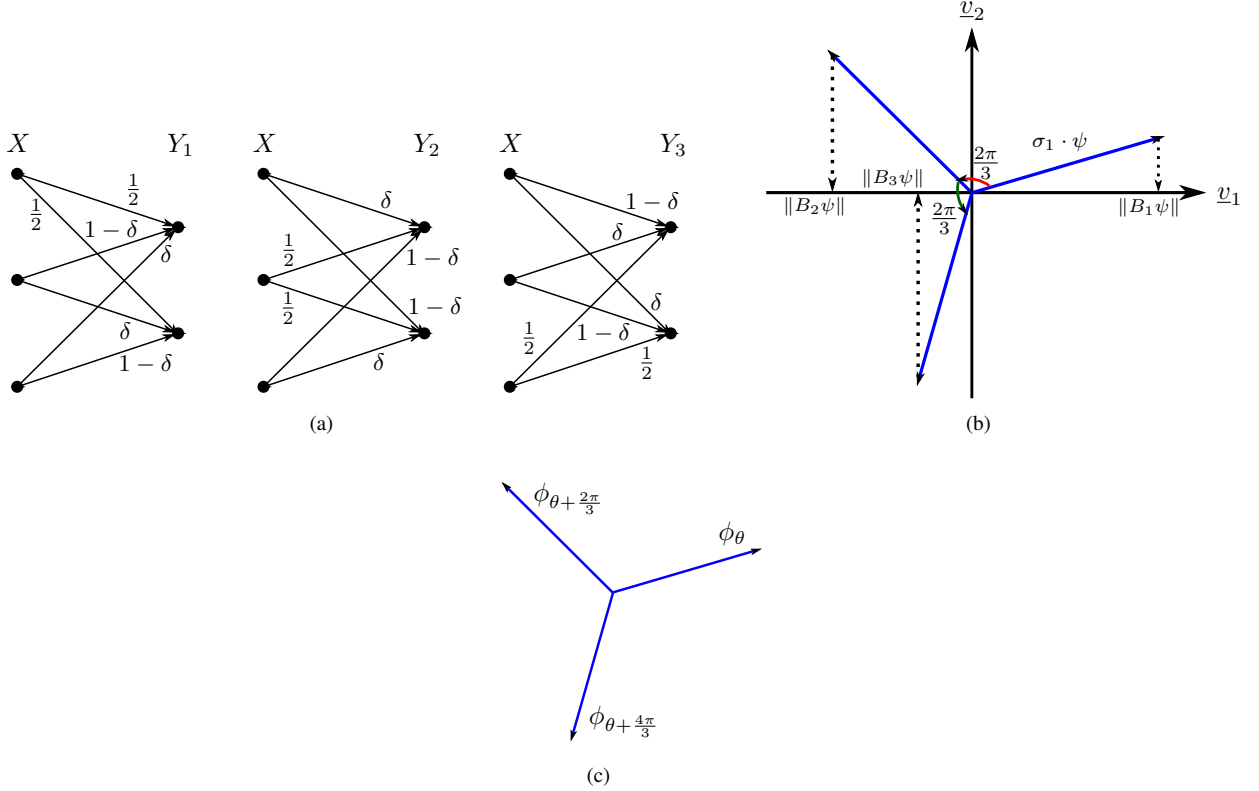


Fig. 6. (a) A ternary input broadcast channel. (b) The lengths of the output images of ψ through matrices B_1, B_2 , and B_3 are the scaled projection of ψ and its rotated version to the horizontal axis. (c) The optimal perturbations over 3 time slots.

then the DTM B_1 for the first receiver Y_1 is

$$B_1 = \sqrt{\frac{2}{3}} \begin{bmatrix} \frac{1}{2} & 1-\delta & \delta \\ \frac{1}{2} & \delta & 1-\delta \end{bmatrix} = \sigma_0 \underline{u}_0 \underline{v}_0^T + \sigma_1 \underline{u}_1 \underline{v}_1^T,$$

where $\sigma_0 = 1$ and $\sigma_1 = \sqrt{\frac{2}{3}}(1-2\delta)$ are the singular values of B_1 , and $\underline{u}_0 = [\frac{1}{\sqrt{2}} \ \frac{1}{\sqrt{2}}]^T$, $\underline{u}_1 = [\frac{1}{\sqrt{2}} \ \frac{-1}{\sqrt{2}}]^T$, $\underline{v}_0 = [\frac{1}{\sqrt{3}} \ \frac{1}{\sqrt{3}} \ \frac{1}{\sqrt{3}}]^T$, and $\underline{v}_1 = [0 \ \frac{1}{\sqrt{2}} \ \frac{-1}{\sqrt{2}}]^T$ are the corresponding left and right singular vectors.

Intuitively, one can think of this channel from the transmitter to the first receiver as a projection operator. It takes the input variation and write it with respect to an orthonormal basis \underline{v}_1 and $\underline{v}_2 = [\frac{2}{\sqrt{6}} \ \frac{-1}{\sqrt{6}} \ \frac{-1}{\sqrt{6}}]^T$, takes the first element along \underline{v}_1 , scales by σ_1 , and maps to the output direction of \underline{u}_1 . The input variation in the direction of \underline{v}_2 is wiped out by the channel, and has no effect to the output distribution.

Similarly, we can write the the DTM's B_2 and B_3 for receivers Y_2 and Y_3 as

$$B_2 = \sqrt{\frac{2}{3}} \begin{bmatrix} \delta & \frac{1}{2} & 1-\delta \\ 1-\delta & \frac{1}{2} & \delta \end{bmatrix} = \sigma_0 \underline{u}_0 \underline{v}_0^T + \sigma_1 \underline{u}_1 [1 \ 0] \begin{bmatrix} \cos \frac{2\pi}{3} & -\sin \frac{2\pi}{3} \\ \sin \frac{2\pi}{3} & \cos \frac{2\pi}{3} \end{bmatrix} \begin{bmatrix} \underline{v}_1^T \\ \underline{v}_2^T \end{bmatrix},$$

and

$$B_3 = \sqrt{\frac{2}{3}} \begin{bmatrix} 1-\delta & \delta & \frac{1}{2} \\ \delta & 1-\delta & \frac{1}{2} \end{bmatrix} = \sigma_0 \underline{u}_0 \underline{v}_0^T + \sigma_1 \underline{u}_1 [1 \ 0] \begin{bmatrix} \cos \frac{4\pi}{3} & -\sin \frac{4\pi}{3} \\ \sin \frac{4\pi}{3} & \cos \frac{4\pi}{3} \end{bmatrix} \begin{bmatrix} \underline{v}_1^T \\ \underline{v}_2^T \end{bmatrix},$$

The channel B_2 also represents the input variation with the orthonormal basis $\underline{v}_1, \underline{v}_2$. However, it rotates the 2-dimensional coefficient vector by $\frac{2\pi}{3}$, before taking the first element, and similarly scales by σ_1 and maps to \underline{u}_1 . The channel B_3 does the same thing, except the rotation is $\frac{4\pi}{3}$. This is illustrated in Figure 6(b), from which the name “windmill” channel should be obvious.

Now if we pick a single input direction ψ , it can be shown that for any ψ with $\|\psi\|^2 = 1$, $\min \{\|B_1\psi\|^2, \|B_2\psi\|^2, \|B_3\psi\|^2\} \leq \frac{1}{4}\sigma_1^2$. To see that, for example if we simply take $\psi = \underline{v}_1$. The output squared norm $\|B_1\psi\|^2$ is σ_1^2 , but $\|B_2\psi\|^2 = \|B_3\psi\|^2 = \frac{1}{4}\sigma_1^2$. A variation from this choice would reduce either $\|B_2\psi\|^2$ or $\|B_3\psi\|^2$, hence further reduce the minimum. The point here is that the largest output $\|B_1\psi\|^2$ is not used.

For a better choice, we take $\mathcal{U} = \{0, 1, 2\}$, with $P_U(u) = 1/3$ for all u . Write

$$\phi_\theta = \cos \theta \cdot \underline{v}_1 + \sin \theta \cdot \underline{v}_2$$

we pick for any θ_0

$$\psi_0 = \phi_{\theta_0}, \quad \psi_1 = \phi_{\theta_0 + \frac{2\pi}{3}}, \quad \psi_2 = \phi_{\theta_0 + \frac{4\pi}{3}}$$

This corresponds to choosing the conditional distributions $P_{X|U=u}(x) = P_X(x) + \epsilon \sqrt{P_X(x)} \psi_u(x)$, $\forall x, u$. It is easy to verify that

$$\sum_u P_U(u) \|B_i \cdot \psi_u\|^2 = \frac{1}{2} \sigma_1^2$$

for all $i = 1, 2, 3$ and regardless of the value of θ_0 .

Equivalently, we can turn this averaging over U into an average over time. To do that, we consider a 3-letter solution to the problem, where we can keep U to be binary, and set

$$P_{X^3|U} = (P_X \pm \epsilon \sqrt{P_X} \psi_0) \otimes (P_X \pm \epsilon \sqrt{P_X} \psi_1) \otimes (P_X \pm \epsilon \sqrt{P_X} \psi_2)$$

where the signs depend on the value of U . This corresponds to perturbations along the vector

$$\psi_0 \otimes \underline{v}_0 \otimes \underline{v}_0 + \underline{v}_0 \otimes \psi_1 \otimes \underline{v}_0 + \underline{v}_0 \otimes \underline{v}_0 \otimes \psi_2$$

The point is that with a $K = 3$ letter solution, we can limit the cardinality of U to be not increasing with the number of receivers K .

Translating this solution to the coding language, the later solution can be interpreted as repeating the binar message U in three time slots. This can be thought as feeding the common information in turn to three individual receivers.

Remark 6. The above analysis can be generalized to general broadcast channels with K receivers. In such problems, there are $2^K - 1$ different types of messages, one to be decoded by a particular subset of $K' \leq K$ receivers. With the same argument that we separated the design of the private messages from the common message in Lemma 3, we can without loss of the optimality separately design the perturbation vectors for each of such messages, which is equivalent as a K' receiver broadcast channel. The overall transmitted codeword is then the superposition of all such messages. It is then modulated on a sequence of i.i.d. P_X symbols as described in section II-D. Each receiver will decode all the messages designated to him. Since all perturbations are local, even the order of decoding these messages can be arbitrary.

This scheme above is by no means designed to achieve the capacity region. The local approximations are so crude that some critical issues in achieving the capacity, such as the order of decoding different messages, have no effect on the approximated performance, and thus can not be addressed with this approach. Moreover, some of observations, such as single-letter solutions are not generally optimal for $K > 2$ receiver channels, have been reported [6], with more general terms. The geometric analysis, however, does help to reveal some issues in a very explicit way, and suggests new directions of designing coding schemes that might be even applicable to the non-local problems, such as using a larger (but finite) cardinality of U to balance the performance between multiple users.

IV. THE MULTIPLE ACCESS CHANNELS WITH COMMON SOURCES

In this section, we want to apply the local geometric approach to the multiple access channel (MAC), and study the corresponding linear information coupling problem. Specifically, we consider the set-up, where the transmitters can not only have the knowledge of their own private sources, but each subset of transmitters also share the knowledge of a common source. In particular, all these private and common sources are assumed to be independent with each other.

The MAC with common sources is a celebrated information theory problem [1], [14]. The main challenge of investigating efficient transmission schemes for common messages lies on modeling the benefit of the collaboration between transmitters that shares common knowledge. This collaboration gain is well studied as the beam-forming gain for Gaussian additive channels; however, for general discrete memoryless MACs, there still lacks a systematic and simple approach to quantitatively compute this gain. In this section, we aim to provide new perspective on understanding the transmitter collaboration gain via our local approach. To illustrate how our technique is applied to this problem, let us first consider the 2-transmitter MAC with the common source.

Suppose that the 2-transmitter multiple access channel has the inputs $X_1 \in \mathcal{X}_1$, $X_2 \in \mathcal{X}_2$, and the output $Y \in \mathcal{Y}$. The memoryless channel is specified by the channel matrix W , where $W(y|x_1, x_2) = P_{Y|X_1, X_2}(y|x_1, x_2)$ is the conditional distribution of the output signals. We want to communicate three messages M_1 , M_2 , and M_0 to the receiver Y with rate R_1 , R_2 , and R_0 , where M_1 and M_2 are privately observed by transmitters 1 and 2, respectively, and both transmitters have the common knowledge on M_0 . Then, following the same arguments as the broadcast channel in section III, the single-letter version of the linear information coupling problem of the MAC is formulated as three sub-problems: the optimization problems

for the private sources M_1 and M_2

$$\begin{aligned} & \max. \quad \frac{1}{n} I(V_i; Y) \\ & \text{subject to: } V_i \rightarrow X_i \rightarrow Y, \frac{1}{n} I(V_i; X_i) \leq \frac{1}{2} \epsilon_i^2, \\ & \quad \frac{1}{n} \|P_{X_i|V_i=v_i} - P_{X_i}\|^2 = O(\epsilon_i^2), \forall v_i. \end{aligned} \quad (46)$$

for $i = 1, 2$, and the optimization problem for the common source M_0

$$\begin{aligned} & \max. \quad \frac{1}{n} I(U; Y) \\ & \text{subject to: } U \rightarrow (X_1, X_2) \rightarrow Y, \frac{1}{n} I(U; X_1, X_2) \leq \frac{1}{2} \epsilon_0^2, \\ & \quad \frac{1}{n} \|P_{X_1, X_2|U=u} - P_{X_1, X_2}\|^2 = O(\epsilon_0^2), \forall u. \end{aligned} \quad (47)$$

Now, let us employ the notations $P_{X_i|V_i=v_i} = P_{X_i} + \epsilon_i \cdot J_{v_i}$ and $P_{X_i|U=u} = P_{X_i} + \epsilon \cdot J_{i,u}$, for $i = 1, 2$, and let ψ denote the scaled perturbation vectors. Then, note that $P_{X_1, X_2|U} = P_{X_1|U} \cdot P_{X_2|U}$ since U is the only common message shared by X_1 and X_2 , the problems (46) and (47) can be simplified to local problems

$$\begin{aligned} & \max. \quad \sum_{v_i} P_{V_i}(v_i) \cdot \|B_i \psi_{v_i}\|^2 \\ & \text{subject to: } \sum_{v_i} P_{V_i}(v_i) \cdot \|\psi_{v_i}\|^2 = 1, \end{aligned} \quad (48)$$

for $i = 1, 2$, and

$$\begin{aligned} & \max. \quad \sum_u P_U(u) \cdot \|B_1 \psi_{1,u} + B_2 \psi_{2,u}\|^2 \\ & \text{subject to: } \sum_u P_U(u) \cdot (\|\psi_{1,u}\|^2 + \|\psi_{2,u}\|^2) = 1. \end{aligned} \quad (49)$$

Here, the DTM B_i is defined as $B_i \triangleq [\sqrt{P_Y}^{-1}] W_i [\sqrt{P_{X_i}}]$, for $i = 1, 2$, with the channel matrix

$$W_i(y|x_i) \triangleq \sum_{x_{3-i} \in \mathcal{X}_{3-i}} W(y|x_1, x_2) P_{X_{3-i}}(x_{3-i}).$$

Remark 7. Compare (46) and (47), the main difference is that when optimizing (47), the perturbation vector can be chosen around the joint distribution P_{X_1, X_2} . On the other hand, the problem (46) is optimized over a projected space, namely, the perturbation vector is only allowed to be designed around the marginal distribution P_{X_i} . Thus, the optimal solution of (47) is larger than (46) due to the more freedom of designing the perturbation vectors over a higher dimensional space. Moreover, the solution of (47) quantitatively illustrates how benefit the collaboration between transmitters is. Therefore, our approach in fact provides a way to visualize the structure the collaboration gain.

In general, the problems (46) and (47) shall be formulated as multi-letter problems. Simplifying to linear algebra problems, the multi-letter version of (46) is precisely the same as the point-to-point problem in section II. On the other hand, the multi-letter version of (47), simplified by taking U as Bernoulli(1/2) random variable⁵, can be written as

$$\max_{\|\psi_{1,u}\|^2 + \|\psi_{2,u}\|^2 = 1} \left\| B_1^{(n)} \cdot \psi_{1,u} + B_2^{(n)} \cdot \psi_{2,u} \right\|^2. \quad (50)$$

In addition, for both $i = 1, 2$, $\psi_{i,u}$ has to be orthogonal to $[\sqrt{P_{X_i}}, x_i \in \mathcal{X}_i]^T$ to guarantee that $P_{X_i|U}$ is a valid probability distribution. This constraint is slightly stronger than the corresponding one in the point-to-point case. Therefore, the verification of the single-letter optimality of (50) is carried out in two steps: 1) we need to show that the second largest singular value of multi-letter linear map $B_{0,n} = [B_1^{(n)} \ B_2^{(n)}]$ is the same as the corresponding single-letter one; 2) we need to demonstrate that the right singular vector of $B_{0,1}$ w.r.t. the second largest singular value satisfies the stronger orthogonality constraint. The following theorem 2 summarizes these two steps for a more general K -user case, and concludes that (50) is in fact single-letter optimal.

Theorem 2. For a multiple access channel with transmitters $1, 2, \dots, k$, let B_i be the corresponding DTM's. Then, the second

⁵Following the same argument as the point-to-point case, this choice of U is indeed without loss of the optimality.

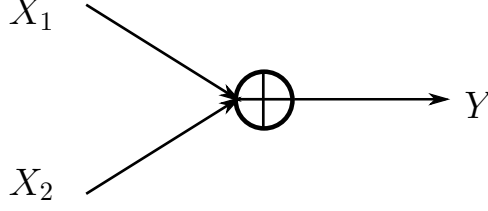


Fig. 7. The binary addition channel with two binary inputs X_1 and X_2 , and the ternary output $Y = X_1 + X_2$.

largest singular value of $B_{0,n} = [B_1^{(n)} \dots B_k^{(n)}]$ is the same as $B_0 \triangleq B_{0,1}$. Moreover, let $\psi_{U=u} = [\psi_1^T \dots \psi_k^T]^T$ be the singular vector of B_0 with the second largest singular value, where ψ_i is an $|\mathcal{X}_i|$ -dimensional vector. Then, ψ_i is orthogonal to $[\sqrt{P_{X_i}}, x_i \in \mathcal{X}_i]^T$, for all $1 \leq i \leq k$.

Example 4. Consider the binary adder channel as shown in Figure 7, where X_1 and X_2 are both binary inputs, and the ternary output $Y = X_1 + X_2$ (the arithmetic addition, not modulo 2). The empirical distribution of both P_{X_1} and P_{X_2} are fixed as $[\frac{1}{2} \ \frac{1}{2}]^T$, and the corresponding output distribution is $[\frac{1}{4} \ \frac{1}{2} \ \frac{1}{4}]^T$. The DTM's for transmitter 1 and 2 are

$$B_1 = B_2 = \begin{bmatrix} \frac{1}{\sqrt{2}} & 0 \\ \frac{1}{2} & \frac{1}{2} \\ 0 & \frac{1}{\sqrt{2}} \end{bmatrix}.$$

Thus, the DTM for the common source is

$$B_0 = \begin{bmatrix} \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} & 0 \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ 0 & \frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} \end{bmatrix}.$$

The second largest singular value of B_0 is 1 with right singular vector $[\frac{1}{2} \ \frac{-1}{2} \ \frac{1}{2} \ \frac{-1}{2}]^T$. In comparison, the second largest singular of both B_1 and B_2 are $\frac{1}{\sqrt{2}}$ with right singular vector $[\frac{1}{\sqrt{2}} \ \frac{-1}{\sqrt{2}}]^T$. Therefore, there is a 3dB *coherent combining gain* that arises from the cooperation between transmitters due to their common knowledge.

Remark 8. It is straight forward to extend the analysis in this section to K -user MAC, in which there are $2^K - 1$ different types of sources, and each source is accessible by a particular subset of transmitters. With a similar argument as the broadcast channel, the optimal perturbation vectors for transmitting each type of message are separately designed, and the corresponding subset of transmitters cooperatively modulate that source into the input symbols. In particular, the cooperation between transmitters increases the efficiency of information transmission, which provides a coherent combining gain, or also called as the beam-forming gain. This gain is quantitatively reflected from the larger singular value of the DTM of the common source as demonstrated in example 4. Finally, the overall transmitted codeword is the superposition of all such sources.

V. CONCLUSION

In this paper, we developed a local approximation approach, which approximates the K-L divergence by a squared Euclidean metric in an Euclidean space. Under the local approximation, we constructed the coordinates and the notion of orthogonality for the probability distribution space. With this approach, we can solve a certain class of information theory problems, which we call the linear information coupling problems, for different types communication channels. We also showed that the single-letterization of multi-terminal problems can be simplified as some linear algebra problems, which can be solved in a systematic way. Moreover, applying our approach to the general broadcast channels, the transmission of the common message can be formulated as the trade-off between multiple linear systems. In order to achieve the optimal trade-off, it is required to code over multiple letters with the number of letters proportional to the number of receivers. Finally, for the multiple access channel with common sources, there exists some coherent combining gains due to the cooperation between transmitters, and we can evaluate this gain quantitatively by using our technique.

The development of this paper can be extended to more general multi-terminal communication networks, such as layered networks. Thus, our approach can be considered as a useful tool to study efficient information flow in networks. Moreover, the coding insights obtained in this paper can be easily carried to designing efficient network communication channel codes. This provides interesting directions for future researches.

APPENDIX A
PROOF OF LEMMA 3

Since U , V_1 , and V_2 are mutually independent, we have

$$\begin{aligned} I(U, V_1, V_2; \underline{X}) &= I(U; \underline{X}) + I(V_1; \underline{X}|U) + I(V_2; \underline{X}|U, V_1) \\ &\geq I(U; \underline{X}) + I(V_1; \underline{X}) + I(V_2; \underline{X}). \end{aligned}$$

Thus, the rate region (39) is belong to (40). On the other hand, for any rate tuple (R_0, R_1, R_2) in (40) achieved by some mutually independent U , V_1 , and V_2 , with $\frac{1}{n}I(U; \underline{X}) \leq \frac{1}{2}\epsilon_0^2$, and $\frac{1}{n}I(V_i; \underline{X}) \leq \frac{1}{2}\epsilon_i^2$ for $i = 1, 2$, where $\sum_{i=1}^3 \epsilon_i^2 = \epsilon^2$, we assume that the conditional distributions achieving this rate tuple have the perturbation forms $P_{\underline{X}|U=u} = P_{\underline{X}} + \sqrt{n}\epsilon_0 \cdot J_u$, and $P_{\underline{X}|V_i=v_i} = P_{\underline{X}} + \sqrt{n}\epsilon_i \cdot J_{v_i}$, for $i = 1, 2$. Then, it is easy to verify that

$$Q_{\underline{X}|(U,V_1,V_2)=(u,v_1,v_2)} = P_{\underline{X}} + \sqrt{n}\epsilon_0 J_u + \sqrt{n}\epsilon_1 J_{v_1} + \sqrt{n}\epsilon_2 J_{v_2}$$

is a valid conditional distribution with marginal $P_{\underline{X}}$. Therefore, using $Q_{\underline{X}|(U,V_1,V_2)=(u,v_1,v_2)}$ as the conditional distribution, the mutual information

$$\begin{aligned} &\frac{1}{n}I(U, V_1, V_2; \underline{X}) \\ &= \frac{1}{2} \sum_{u,v_1,v_2} P_U(u)P_{V_1}(v_1)P_{V_2}(v_2) \cdot \|\epsilon_0 J_u + \epsilon_1 J_{v_1} + \epsilon_2 J_{v_2}\|_{P_X}^2 + o(\epsilon^2) \\ &\leq \frac{1}{2} (\epsilon_0^2 + \epsilon_1^2 + \epsilon_2^2) + o(\epsilon^2) = \frac{1}{2}\epsilon^2 + o(\epsilon^2), \end{aligned} \tag{51}$$

where (51) is resulted from the definition of the perturbation vectors:

$$\sum_u P_U(u)J_u = 0, \quad \sum_{v_i} P_{V_i}(v_i)J_{v_i} = 0, \quad \text{for } i = 1, 2,$$

and

$$\begin{aligned} \sum_u P_U(u) \|J_u\|_{P_X}^2 &\leq 1, \\ \sum_{v_i} P_{V_i}(v_i) \|J_{v_i}\|_{P_X}^2 &\leq 1, \quad \text{for } i = 1, 2. \end{aligned}$$

Hence, we can take $Q_{\underline{X}|(U,V_1,V_2)=(u,v_1,v_2)}$ as the conditional distribution in (39), and obtain a rate tuple that is equal to (R_0, R_1, R_2) , up to the first order approximation.

APPENDIX B
PROOF OF THEOREM 1

The part a) and b) of Theorem 1 are directly followed from the following lemma.

Lemma 4 (Optimal solutions have product forms). *For any $n \geq K$, there exist $|\mathcal{X}|$ -dimensional vectors $\underline{v}_1^*, \underline{v}_2^*, \dots, \underline{v}_K^*$, which satisfy $\sum_{u=1}^K \|\underline{v}_u^*\|^2 = 1$, and $\langle \underline{v}_0, \underline{v}_i^* \rangle = 0$, for $u = 1, 2, \dots, K$, such that*

$$\psi_u = \underline{v}_0^{(n-K)} \otimes \left(\underline{v}_0^{(u-1)} \otimes \underline{v}_u^* \otimes \underline{v}_0^{(K-u)} \right), \tag{52}$$

and $|\mathcal{U}| = K$ with $P_U(u) = 1/K$ is an optimal solution of (45). Here, $\underline{v}_0^{(\cdot)}$ is the Kronecker product of \underline{v}_0 .

In order to prove lemma 4, we need to first establish the following lemma 5, which illustrates the required degree of freedom for describing the optimal tradeoff between multiple linear systems.

Lemma 5. *Assume that $\Theta_i = \text{diag}\{\theta_{i,1}, \theta_{i,2}, \dots, \theta_{i,M}\}$, for $i = 1, 2, \dots, k$, if the optimization problem*

$$\begin{aligned} &\max. \quad \|\Theta_k \cdot \underline{c}\|^2 \\ &\text{subject to:} \quad \|\underline{c}\|^2 = 1, \text{ and } \|\Theta_i \cdot \underline{c}\|^2 = \lambda_i, \\ &\quad \text{for } i = 1, 2, \dots, k-1, \end{aligned} \tag{53}$$

has global optimal solutions, then there exists a global optimal solution $\underline{c}^* = [c_1^* \ c_2^* \ \dots \ c_M^*]^T$ with at most k nonzero entries.

Proof of Lemma 5: Let us assume that $\underline{c}^* = [c_1^* \ c_2^* \ \dots \ c_M^*]^T$ is the global optimal solution of (53) with the least number of nonzero entries l . If $l > k$, then without loss of generality, we can assume that $c_i \neq 0$ for $i \leq l$, and $c_i = 0$ for $i > l$.

For $i = 0, 1, \dots, k$, define the vector $\underline{\theta}_{i,l} = [\theta_{i,1}^2 \ \theta_{i,2}^2 \ \dots \ \theta_{i,l}^2]^T \in \mathbb{R}^l$, and $\underline{\theta}_{0,l} = [1 \ \dots \ 1]^T \in \mathbb{R}^l$, then the null space $\text{Null}(\underline{\theta}_{i,l}) \subset \mathbb{R}^l$ has dimension at least $l - 1$, and the space of the intersecting of null spaces $\cup_{i=0}^{k-1} \text{Null}(\underline{\theta}_{i,l})$ has dimension at least $l - k > 0$. Let the nonzero vector $\underline{d} = [d_1 \ d_2 \ \dots \ d_l]^T \in \cup_{i=0}^{k-1} \text{Null}(\underline{\theta}_{i,l})$, and $\underline{c}_t = [c_{1,t} \ \dots \ c_{l,t} \ 0 \ \dots \ 0]^T \in \mathbb{R}^m$, where $c_{i,t} = \sqrt{c_i^{*2} + t \cdot d_i}$. Since \underline{c}^* is a global optimal, we have $\frac{\partial \|\Theta_k \cdot \underline{c}_t\|^2}{\partial t} = 0$, which implies that $\langle \underline{\theta}_{k,l}, \underline{d} \rangle = 0$. Thus, if we take $t^* \triangleq \max \{t : c_i^{*2} + t \cdot d_i \geq 0, \forall 1 \leq i \leq l\}$, then \underline{c}_{t^*} is a global optimal solution with at most $l - 1$ nonzero entries, which contradicts to the assumption of \underline{c}^* . Therefore, \underline{c}^* has at most k nonzero entries. ■

Lemma 5 immediately implies the following Corollary.

Corollary 1. Assume that $\Theta_i = \text{diag} \{\theta_{i,1}, \theta_{i,2}, \dots, \theta_{i,M}\}$, for $i = 1, 2, \dots, k$, then the optimization problem

$$\max_{\|\underline{c}\|^2=1} \min_{1 \leq i \leq k} \{\|\Theta_i \cdot \underline{c}\|^2\} \quad (54)$$

has a global optimal solution $\underline{c}^* = [c_1^* \ c_2^* \ \dots \ c_M^*]^T$ with at most k nonzero entries.

Now, let us prove Lemma 4. For the sake of presentation convenience, we demonstrate here the proof of the case $K = 2$, while this technique can be carried out to general K -user case without difficulty.

Proof of Lemma 4: Let $\sigma_0 = 1, \sigma_1, \dots, \sigma_m$ and $\mu_0 = 1, \mu_1, \dots, \mu_m$ be the singular values of the DTM's B_1 and B_2 , respectively, and the corresponding right singular vectors are $\underline{v}_0, \underline{v}_1, \dots, \underline{v}_m$ and $\underline{u}_0, \underline{u}_1, \dots, \underline{u}_m$, where $m \triangleq |\mathcal{X}| - 1$, and $\underline{v}_0 = \underline{u}_0 = [\sqrt{P_X}, x \in \mathcal{X}]^T$. Moreover, we assume that $\underline{v}_i = \sum_{k=0}^m \phi_{ik} \underline{u}_k$, where $\Phi_0 = [\phi_{ij}]_{i,j=0}^m$ is an $|\mathcal{X}|$ -by- $|\mathcal{X}|$ unitary matrix. Then, we have $\phi_{00} = 1$, $\phi_{i0} = \phi_{0i} = 0$, for all $i > 0$.

Now for any $n \geq K$, our goal here is to show that for any choice of ψ'_u satisfying the constraints of (45), we can always find a set of ψ_u taking product form (52) that has no smaller output image in (45). The first observation here is that we can only restrict our focus on the ψ'_u 's such that all the ψ'_u 's are mutually orthogonal. The reason is that we can construct mutually orthogonal vectors $\psi''_u = \underline{v}_0^{((u-1) \cdot n)} \otimes \psi'_u \otimes \underline{v}_0^{((|U|-u) \cdot n)}$, and alternatively prove lemma 4 for ψ''_u . Now, for mutually orthogonal vectors ψ'_u , let us write ψ' as

$$\psi' = \sum_u \sqrt{P_U(u)} \cdot \psi_u.$$

Then, the output images of (45) becomes $\|B_i^{(n)} \cdot \psi'\|$, for $i = 1, 2$, with the constraint $\|\psi'\| = 1$, and $\langle \psi', \underline{v}_0^{(n)} \rangle = 0$.

Now, suppose that

$$\begin{aligned} \psi' &= \sum_{\substack{i_1, \dots, i_n=0 \\ (i_1, \dots, i_n) \neq (0, \dots, 0)}}^m \alpha_{i_1 \dots i_n} \cdot (\underline{v}_{i_1} \otimes \dots \otimes \underline{v}_{i_n}) \\ &= \sum_{j_1, \dots, j_n=0}^m \beta_{j_1 \dots j_n} \cdot (\underline{u}_{j_1} \otimes \dots \otimes \underline{u}_{j_n}), \end{aligned}$$

where

$$\beta_{j_1 \dots j_n} = \sum_{\substack{i_1, \dots, i_n=0 \\ (i_1, \dots, i_n) \neq (0, \dots, 0)}}^m \alpha_{i_1 \dots i_n} \phi_{i_1 j_1} \dots \phi_{i_n j_n}.$$

Then, since $\|\psi'\| = 1$, we have

$$\sum_{\substack{i_1, \dots, i_n=0 \\ (i_1, \dots, i_n) \neq (0, \dots, 0)}}^m \|\alpha_{i_1 \dots i_n}\|^2 = \sum_{j_1, \dots, j_n=0}^m \|\beta_{j_1 \dots j_n}\|^2 = 1.$$

Now, let us define

$$\mathcal{S}_k = \{(i_1, \dots, i_n) : 0 \leq i_a \leq m, \forall 1 \leq a \leq n, \\ i_k \neq 0, i_{k+1} = \dots = i_n = 0\},$$

$$\mathcal{T}_k = \{(i_1, \dots, i_k) : 0 \leq i_a \leq m, \forall 1 \leq a \leq k\},$$

with $\mathcal{T}_0 = \emptyset$, $\mathcal{T} = \cup_{k=0}^{n-1} \mathcal{T}_k$, and

$$\xi : \mathcal{T} \mapsto \{1, 2, \dots, M\}$$

is a bijective map, where $M = |\mathcal{T}|$. Then,

$$\begin{aligned}
\|B_1^{(n)} \cdot \psi'\|^2 &= \sum_{\substack{i_1, \dots, i_n=0 \\ (i_1, \dots, i_n) \neq (0, \dots, 0)}}^m \alpha_{i_1 \dots i_n}^2 \sigma_{i_1}^2 \cdots \sigma_{i_n}^2 \leq \sum_{k=1}^n \sum_{(i_1, \dots, i_n) \in \mathcal{S}_k} \alpha_{i_1 \dots i_n}^2 \sigma_{i_k}^2 \\
&= \sum_{k=1}^n \sum_{(i_1, \dots, i_{k-1}) \in \mathcal{T}_{k-1}} \sum_{i_k=1}^m \alpha_{i_1 \dots i_{k-1} i_k 0 \dots 0}^2 \sigma_{i_k}^2 \\
&= \sum_{k=1}^n \sum_{(i_1, \dots, i_{k-1}) \in \mathcal{T}_{k-1}} \|\Sigma \cdot \underline{\alpha}_{\xi(i_1, \dots, i_{k-1})}\|^2 \\
&= \sum_{i=1}^M \|\Sigma \cdot \underline{\alpha}_i\|^2,
\end{aligned}$$

where $\Sigma = \text{diag}\{\sigma_1, \dots, \sigma_m\}$, and $\underline{\alpha}_{\xi(i_1, \dots, i_{k-1})}$ is defined as

$$\underline{\alpha}_{\xi(i_1, \dots, i_{k-1})} = [\alpha_{i_1 \dots i_{k-1} 1 0 \dots 0} \ \alpha_{i_1 \dots i_{k-1} 2 0 \dots 0} \cdots \alpha_{i_1 \dots i_{k-1} m 0 \dots 0}]^T.$$

Moreover,

$$\begin{aligned}
\|B_2^{(n)} \cdot \psi'\|^2 &= \sum_{j_1, \dots, j_n=0}^m \beta_{j_1 \dots j_n}^2 \mu_{j_1}^2 \cdots \mu_{j_n}^2 \\
&= \sum_{j_1, \dots, j_n=0}^m \mu_{j_1}^2 \cdots \mu_{j_n}^2 \cdot \left(\sum_{k=1}^n \sum_{(i_1, \dots, i_n) \in \mathcal{S}_k} \alpha_{i_1 \dots i_n} \phi_{i_1 j_1} \cdots \phi_{i_n j_n} \right)^2 \\
&= \sum_{k=1}^n \sum_{j_1, \dots, j_n=0}^m \mu_{j_1}^2 \cdots \mu_{j_n}^2 \cdot \left(\sum_{(i_1, \dots, i_n) \in \mathcal{S}_k} \alpha_{i_1 \dots i_n} \phi_{i_1 j_1} \cdots \phi_{i_n j_n} \right)^2, \tag{55}
\end{aligned}$$

where (55) is because for any $1 \leq k_1 < k_2 \leq n$,

$$\begin{aligned}
&\sum_{j_1, \dots, j_n=0}^m \left(\sum_{(i_1, \dots, i_n) \in \mathcal{S}_{k_1}} \alpha_{i_1 \dots i_n} \phi_{i_1 j_1} \cdots \phi_{i_n j_n} \right) \cdot \left(\sum_{(i_1, \dots, i_n) \in \mathcal{S}_{k_2}} \alpha_{i_1 \dots i_n} \phi_{i_1 j_1} \cdots \phi_{i_n j_n} \right) \mu_{j_1}^2 \cdots \mu_{j_n}^2 \\
&= \sum_{j_1, \dots, j_n=0}^m \sum_{\substack{(i_1, \dots, i_{k_1}, 0, \dots, 0) \in \mathcal{S}_{k_1} \\ (i'_1, \dots, i'_{k_2}, 0, \dots, 0) \in \mathcal{S}_{k_2}}} \alpha_{i_1 \dots i_{k_1} 0 \dots 0} \alpha_{i'_1 \dots i'_{k_2} 0 \dots 0} \cdot (\phi_{i_1 j_1} \phi_{i'_1 j_1}) \cdots \underbrace{(\phi_{0 j_{k_2}} \phi_{i'_{k_2} j_{k_2}})}_{\text{nonzero only if } j_{k_2} = i'_{k_2} = 0, \text{ but } i'_{k_2} \neq 0} \mu_{j_1}^2 \cdots \mu_{j_n}^2 \\
&= 0
\end{aligned}$$

Then, let $\Omega = \text{diag}\{\mu_1, \dots, \mu_m\}$ and $\Phi = [\phi_{ij}]_{i,j=1}^m$, for each k , we have

$$\begin{aligned}
&\sum_{j_1, \dots, j_n=0}^m \left(\sum_{(i_1, \dots, i_n) \in \mathcal{S}_k} \alpha_{i_1 \dots i_n} \phi_{i_1 j_1} \cdots \phi_{i_n j_n} \right)^2 \mu_{j_1}^2 \cdots \mu_{j_n}^2 \\
&\leq \sum_{j_1, \dots, j_n=0}^m \left(\sum_{(i_1, \dots, i_n) \in \mathcal{S}_k} \alpha_{i_1 \dots i_n} \phi_{i_1 j_1} \cdots \phi_{i_n j_n} \right)^2 \mu_{j_k}^2 \\
&= \sum_{j_1, \dots, j_n=0}^m \sum_{(i_1, \dots, i_n) \in \mathcal{S}_k} \sum_{(i'_1, \dots, i'_n) \in \mathcal{S}_k} \alpha_{i_1 \dots i_n} \alpha_{i'_1 \dots i'_n} \cdot (\phi_{i_1 j_1} \phi_{i'_1 j_1}) \cdots (\phi_{i_n j_n} \phi_{i'_n j_n}) \mu_{j_k}^2 \\
&= \sum_{j_k=0}^m \sum_{(i_1, \dots, i_{k-1}) \in \mathcal{T}_{k-1}} \left(\sum_{i_k=1}^m \alpha_{i_1 \dots i_{k-1} i_k 0 \dots 0} \phi_{i_k j_k} \right)^2 \mu_{j_k}^2 \\
&= \sum_{(i_1, \dots, i_{k-1}) \in \mathcal{T}_{k-1}} \|\Omega \Phi^T \underline{\alpha}_{\xi(i_1, \dots, i_{k-1})}\|^2, \tag{56}
\end{aligned}$$

where (56) is because Φ is a unitary matrix, and

$$\sum_{j_r=0}^m \phi_{i_r j_r} \phi_{i'_r j_r} = \begin{cases} 1 & \text{if } i_r = i'_r \\ 0 & \text{otherwise} \end{cases}.$$

Therefore, (55) becomes

$$\|B_2^{(n)} \cdot \psi'\|^2 \leq \sum_{k=1}^n \sum_{(i_1, \dots, i_{k-1}) \in \mathcal{T}_{k-1}} \|\Omega \Phi^T \underline{\alpha}_{\xi(i_1, \dots, i_{k-1})}\|^2 = \sum_{i=1}^M \|\Omega \Phi^T \underline{\alpha}_i\|^2.$$

Now, let us define $\Theta_1 = \text{diag}\{\theta_{1,1}, \dots, \theta_{1,M}\}$, and $\Theta_2 = \text{diag}\{\theta_{2,1}, \dots, \theta_{2,M}\}$ as

$$\theta_{1,i} = \begin{cases} \frac{\|\Sigma \underline{\alpha}_i\|}{\|\underline{\alpha}_i\|} & \text{if } \|\underline{\alpha}_i\| \neq 0 \\ 0 & \text{otherwise} \end{cases},$$

$$\theta_{2,i} = \begin{cases} \frac{\|\Omega \Phi^T \underline{\alpha}_i\|}{\|\Phi^T \cdot \underline{\alpha}_i\|} & \text{if } \|\Phi^T \cdot \underline{\alpha}_i\| \neq 0 \\ 0 & \text{otherwise} \end{cases}.$$

Then, from Corollary 1, there exists an optimal solution \underline{c}^* of the optimization problem

$$\max_{\underline{c} \in \mathbb{R}^M: \|\underline{c}\|^2=1} \min \{ \|\Theta_1 \cdot \underline{c}\|^2, \|\Theta_2 \cdot \underline{c}\|^2 \}, \quad (57)$$

with at most two nonzero entries. Let the i_1 -th entry $c_{i_1}^*$ and the i_2 -th entry $c_{i_2}^*$ of \underline{c}^* are nonzero. Note that $\|\underline{\alpha}_i\| = \|\Phi^T \cdot \underline{\alpha}_i\|$, for all $1 \leq i \leq M$, and

$$\sum_{i=1}^M \|\underline{\alpha}_i\|^2 = \sum_{\substack{i_1, \dots, i_n=0 \\ (i_1, \dots, i_n) \neq (0, \dots, 0)}}^m \|\alpha_{i_1 \dots i_n}\|^2 = 1,$$

thus the vector $\underline{\alpha} = [\|\underline{\alpha}_1\| \ \|\underline{\alpha}_2\| \ \dots \ \|\underline{\alpha}_M\|]^T$ has unit norm. This implies that

$$\begin{aligned} & \min \{ \|\Theta_1 \cdot \underline{c}^*\|^2, \|\Theta_2 \cdot \underline{c}^*\|^2 \} \\ & \geq \min \{ \|\Theta_1 \cdot \underline{\alpha}\|^2, \|\Theta_2 \cdot \underline{\alpha}\|^2 \} \\ & = \min \left\{ \sum_{i=1}^M \|\Sigma \underline{\alpha}_i\|^2, \sum_{i=1}^M \|\Omega \Phi^T \underline{\alpha}_i\|^2 \right\} \\ & = \min \{ \|B_1^{(n)} \cdot L\|^2, \|B_2^{(n)} \cdot L\|^2 \}. \end{aligned}$$

Now, let us take vectors $\underline{v}_1^* = c_{i_1}^* \cdot \sum_{j=1}^m \frac{\alpha_{i_1}(j)}{\|\underline{\alpha}_{i_1}\|} \underline{v}_j$, and $\underline{v}_2^* = c_{i_2}^* \cdot \sum_{j=1}^m \frac{\alpha_{i_2}(j)}{\|\underline{\alpha}_{i_2}\|} \underline{v}_j$, where $\alpha_{i_1}(j)$ and $\alpha_{i_2}(j)$ are the j -th entries of $\underline{\alpha}_{i_1}$ and $\underline{\alpha}_{i_2}$, respectively. Then, the vector $\psi^* = \underline{v}_0^{(n-2)} \otimes (\underline{v}_1^* \otimes \underline{v}_0 + \underline{v}_0 \otimes \underline{v}_2^*)$ satisfies $\|\psi^*\| = 1$, and

$$\begin{aligned} & \min \{ \|B_1^{(n)} \cdot \psi^*\|^2, \|B_2^{(n)} \cdot \psi^*\|^2 \} \\ & = \min \{ \|\Theta_1 \cdot \underline{c}^*\|^2, \|\Theta_2 \cdot \underline{c}^*\|^2 \} \\ & \geq \min \{ \|B_1^{(n)} \cdot \psi'\|^2, \|B_2^{(n)} \cdot \psi'\|^2 \}. \end{aligned}$$

Therefore, by taking $\psi_i = \underline{v}_0^{(n-2)} \otimes \underline{v}_i^* \otimes \underline{v}_0$ for $i = 1, 2$ in (52), we come up with vectors with product form and no smaller output images. This proves lemma 4. \blacksquare

Now, in order to prove part c), we only need to show that for $K = 2$, $\sup_n \lambda_B^{(n)} = \lambda_B^{(1)}$. Equivalently, we will show that there exists a unit vector ψ such that $\sup_n \lambda_B^{(n)} = \|B^{(1)} \cdot \psi\|$. For this purpose, let us start from an optimal solution $\psi^* = \underline{v}_1 \otimes \underline{v}_0 + \underline{v}_0 \otimes \underline{v}_2$ of (45), where $\underline{v}_1 = \sum_{j=1}^m a_j \cdot \underline{v}_j$, and $\underline{v}_2 = \sum_{j=1}^m b_j \cdot \underline{v}_j$, and $\|\underline{v}_1\|^2 + \|\underline{v}_2\|^2 = 1$. Let $\underline{a} = [a_1 \ \dots \ a_m]^T$ and $\underline{b} = [b_1 \ \dots \ b_m]^T$, then,

$$\begin{aligned} & \min \{ \|B_1^{(2)} \cdot L_2\|^2, \|B_2^{(2)} \cdot L_2\|^2 \} \\ & = \min \{ \|\Sigma \underline{a}\|^2 + \|\Sigma \underline{b}\|^2, \|\Omega \Phi^T \underline{a}\|^2 + \|\Omega \Phi^T \underline{b}\|^2 \} \end{aligned}$$

Our goal is to show that there exists a unit vector $\underline{c} = [c_1 \dots c_m]^T$ such that

$$\begin{cases} \|\Sigma \underline{c}\|^2 \geq \|\Sigma \underline{a}\|^2 + \|\Sigma \underline{b}\|^2, \\ \|\Omega \Phi^T \underline{c}\|^2 \geq \|\Omega \Phi^T \underline{a}\|^2 + \|\Omega \Phi^T \underline{b}\|^2. \end{cases} \quad (58)$$

Then, taking $\psi = \sum_{j=1}^m c_j \cdot \underline{v}_j$, and we are done.

Now for $m = 2$, we want to consider the vectors $\underline{c}_1 = [\sqrt{a_1^2 + b_1^2} \ \sqrt{a_2^2 + b_2^2}]^T$, and $\underline{c}_2 = [\sqrt{a_1^2 + b_1^2} \ -\sqrt{a_2^2 + b_2^2}]^T$. Obviously, $\|\Sigma \underline{c}_1\|^2 = \|\Sigma \underline{c}_2\|^2 = \|\Sigma \underline{a}\|^2 + \|\Sigma \underline{b}\|^2$. Note that

$$\begin{aligned} & (\|\Omega \Phi^T \underline{a}\|^2 + \|\Omega \Phi^T \underline{b}\|^2 - \|\Omega \Phi^T \underline{c}_1\|^2) \cdot (\|\Omega \Phi^T \underline{a}\|^2 + \|\Omega \Phi^T \underline{b}\|^2 - \|\Omega \Phi^T \underline{c}_2\|^2) \\ &= -4(a_1 b_2 - b_1 a_2)^2 \cdot (\phi_{11} \phi_{21} \mu_1^2 + \phi_{12} \phi_{22} \mu_2^2) \leq 0 \end{aligned}$$

Therefore, at least one of \underline{c}_1 and \underline{c}_2 satisfies (58).

On the other hand, for $m > 2$, let $A = [\underline{a} \ \underline{b}]$, and consider the SVD of matrices $\Sigma A = U_1^T \Sigma_1 V_1$, and $\Omega \Phi^T A = U_2^T \Sigma_2 V_2$, where V_i is a 2×2 unitary matrix, and Σ_i is a diagonal matrix, for $i = 1, 2$. Moreover, we denote $V_1 = [\varphi_1 \ \varphi_2]$, and $V_2 = [\eta_1 \ \eta_2]$, where φ_i and η_i are all two dimensional unit vectors. Then, $\|\Sigma \underline{a}\|^2 = \|\Sigma_1 \varphi_1\|^2$, $\|\Sigma \underline{b}\|^2 = \|\Sigma_1 \varphi_2\|^2$, and $\|\Omega \Phi^T \underline{a}\|^2 = \|\Sigma_2 (V_2 V_1^{-1}) \eta_1\|^2$, $\|\Omega \Phi^T \underline{b}\|^2 = \|\Sigma_2 (V_2 V_1^{-1}) \eta_2\|^2$. Since $V_2 V_1^{-1}$ is a unitary matrix, there exists a two dimensional unit vector \underline{c}' , such that

$$\begin{cases} \|\Sigma_1 \underline{c}'\|^2 \geq \|\Sigma_1 \varphi_1\|^2 + \|\Sigma_1 \varphi_2\|^2, \\ \|\Sigma_2 (V_2 V_1^{-1}) \underline{c}'\|^2 \geq \|\Sigma_2 (V_2 V_1^{-1}) \eta_1\|^2 + \|\Sigma_2 (V_2 V_1^{-1}) \eta_2\|^2. \end{cases}$$

Now, taking $\underline{c} = A V_1^{-1} \underline{c}'$, then $\|\Sigma \underline{c}\|^2 = \|\Sigma_1 \underline{c}'\|^2$, and $\|\Omega \Phi^T \underline{c}\|^2 = \|\Sigma_2 (V_2 V_1^{-1}) \underline{c}'\|^2$, which implies that \underline{c} satisfies (58).

APPENDIX C PROOF OF THEOREM 2

In order to prove Theorem 2, we will show that:

- 1) the second largest singular value of $B_{0,n} = [B_1^{(n)} \dots B_k^{(n)}]$ is the same as B_0
- 2) ψ_i is orthogonal to $[\sqrt{P_{X_i}}, x_i \in \mathcal{X}_i]^T$, for all $1 \leq i \leq k$.

First, let us prove 1). Suppose that $\sigma_{1,n}$ is the second largest singular value of $B_{0,n}$, then we want to show that $\sigma_{1,n} = \sigma_{1,1}$, for all $n > 1$. Let us first show that $\sigma_{1,2} = \sigma_{1,1}$. Observe that $[\sqrt{P_Y}, y \in \mathcal{Y}]^T$ is the left singular vector of B_0 , corresponding to the largest singular value \sqrt{k} , thus we can assume that the singular values of B_0 are $\sigma_{0,1} = \sqrt{k} \geq \sigma_{1,1} \geq \sigma_{2,1} \geq \dots \geq \sigma_{m,1}$, and the corresponding left singular vectors are $\underline{w}_0 = [\sqrt{P_Y}, y \in \mathcal{Y}]^T$, $\underline{w}_1, \underline{w}_2, \dots, \underline{w}_m$, where $m \triangleq \min \left\{ \sum_{i=1}^k |\mathcal{X}_i|, |\mathcal{Y}| \right\} - 1$. Note that for all $0 \leq i \leq m$,

$$\begin{aligned} & (\underline{w}_0 \otimes \underline{w}_i)^T \cdot (B_{0,2} B_{0,2}^T) \\ &= (\underline{w}_0^T \otimes \underline{w}_i^T) \cdot (B_1 B_1^T \otimes B_1 B_1^T + B_2 B_2^T \otimes B_2 B_2^T) \\ &= \underline{w}_0^T \otimes [\underline{w}_i^T \cdot (B_1 B_1^T + B_2 B_2^T)] \\ &= \underline{w}_0^T \otimes [\underline{w}_i^T \cdot (B_0 B_0^T)] = \sigma_{i,1}^2 \cdot \underline{w}_0^T \otimes \underline{w}_i^T, \end{aligned}$$

therefore, $\underline{w}_0 \otimes \underline{w}_i$ is a singular vector of $B_{0,2}$, with singular value $\sigma_{i,1}$. Similarly, $\underline{w}_j \otimes \underline{w}_0$ is a singular vector of $B_{0,2}$, with singular value $\sigma_{j,1}$, for all $0 \leq j \leq m$. Hence, in order to show that $\sigma_{1,2} = \sigma_{1,1}$, we only need to show that for any unit vector $\underline{w} \in \text{span} \{ \underline{w}_i \otimes \underline{w}_j, 1 \leq i, j \leq m \}$, $\|\underline{w}^T \cdot B_{0,2}\| \leq \sigma_{1,2}$. To this end, note that $\|\underline{w}^T \cdot (B_0 \otimes B_0)\| \leq \sigma_{1,2}^2$, therefore

$$\begin{aligned} \|\underline{w}^T \cdot B_{0,2}\|^2 &\leq \|\underline{w}^T \cdot B_{0,2}\|^2 + \|\underline{w}^T \cdot (B_1 \otimes B_2)\|^2 + \|\underline{w}^T \cdot (B_2 \otimes B_1)\|^2 \\ &= \|\underline{w}^T \cdot (B_0 \otimes B_0)\|^2 \leq \sigma_{1,2}^4 \leq \sigma_{1,2}^2. \end{aligned}$$

Thus, we have $\sigma_{1,2} = \sigma_{1,1}$. With the same arguments, we can show that for any positive integer N , $\sigma_{1,2^N} = \sigma_{1,1}$. Since $\sigma_{1,n}$ is non-decreasing with n , this implies that $\sigma_{1,n} = \sigma_{1,1}$, for all n .

Now, let us prove the statement (ii). For simplicity, we denote $\underline{v}_{i,0} = [\sqrt{P_{X_i}}, x_i \in \mathcal{X}_i]^T$, and $\underline{v} = [\underline{v}_{1,0}^T \dots \underline{v}_{k,0}^T]^T$, then \underline{v} is the singular vector of B_0 , corresponding to the largest singular value \sqrt{k} . Suppose that $\langle \psi_i, \underline{v}_{i,0} \rangle = \mathbb{I}_i$, since $\psi_{U=u}$ is orthogonal to \underline{v} , we have $\sum_{i=1}^k \mathbb{I}_i = 0$. Now, if there exists a j such that $\mathbb{I}_j \neq 0$, then define the vector $\tilde{\psi}_{U=u} = [\tilde{\psi}_1^T \dots \tilde{\psi}_k^T]^T$, where $\tilde{\psi}_i = (\psi_i - \mathbb{I}_i \cdot \underline{v}_i) / \sqrt{1 - \mathbb{I}_i^2}$, and $\mathbb{I} = \sum_{i=1}^k \mathbb{I}_i^2 > 0$. This definition of $\tilde{\psi}_u$ is valid because $\mathbb{I} < \sum_{i=1}^k \|\psi_i\|^2 = 1$. Then,

it is easy to verify that $\|\tilde{\psi}_{U=u}\| = 1$, and $\tilde{\psi}_{U=u}$ is orthogonal to \underline{v} . Moreover,

$$\begin{aligned} B_0 \cdot \tilde{\psi}_{U=u} &= \sqrt{1 - \mathbb{I}}^{-1} \cdot \left(B_0 \cdot \psi_{U=u} - \sum_{i=1}^k \mathbb{I}_i \cdot (B_i \cdot \underline{v}_{i,0}) \right) \\ &= \sqrt{1 - \mathbb{I}}^{-1} \cdot \left(B_0 \cdot \psi_{U=u} - \left(\sum_{i=1}^k \mathbb{I}_i \right) \cdot \underline{w}_0 \right) \\ &= \sqrt{1 - \mathbb{I}}^{-1} \cdot (B_0 \cdot \psi_{U=u}), \end{aligned}$$

where $\underline{w}_0 = [\sqrt{P_Y}, y \in \mathcal{Y}]^T$. Therefore, $\|B_0 \cdot \tilde{\psi}_{U=u}\| > \|B_0 \cdot \psi_{U=u}\|$, since $\mathbb{I} > 0$. This contradicts to the assumption that $\psi_{U=u}$ is the singular vector of B_0 , corresponding to the second largest singular value. Thus, ψ_i is orthogonal to $[\sqrt{P_{X_i}}, x_i \in \mathcal{X}_i]^T$, for all $1 \leq i \leq k$.

REFERENCES

- [1] T. M. Cover and J. A. Thomas, *Elementary of Information Theory*, Wiley Interscience, 1991.
- [2] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*, New York: Academic, 1981.
- [3] A. El Gamal and Y. Kim, *Network Information Theory*, Cambridge University Press, 2012.
- [4] Shun-ichi Amari and Hiroshi Nagaoka, *Methods of Information Geometry*, Oxford University Press, 2000.
- [5] T. M. Cover, "An Achievable Rate Region for the Broadcast Channel," *IEEE Transactions on Information Theory*, Vol. IT-21, pp. 399-404, July, 1975.
- [6] C. Nair and A. El Gamal, "The Capacity Region of a Class of Three-Receiver Broadcast Channels With Degraded Message Sets," *IEEE Transactions on Information Theory*, Vol. IT-55, pp. 4479-4493, Oct., 2009.
- [7] S. Borade and L. Zheng, "Euclidean Information Theory," *IEEE International Zurich Seminars on Communications*, March, 2008.
- [8] E. Erkip and T. M. Cover, "The Efficiency of Investment Information," *IEEE Transactions on Information Theory*, Vol. IT-44, pp. 1026-1040, May, 1998.
- [9] H. O. Hirschfeld, "A connection between correlation and contingency," *Proc. Cambridge Philosophical Soc.*, Vol. 31, pp. 520-524, 1935.
- [10] H. Gebelein, "Das statistische problem der Korrelation als variations-und Eigenwertproblem und sein Zusammenhang mit der Ausgleichungsrechnung," *Z. für angewandte Math. und Mech.*, Vol. 21, pp. 364-379, 1941.
- [11] A. Rényi, "New version of the probabilistic generalization of the large sieve," *Acta Math. Hung.*, Vol. 10, pp. 217-226, 1959.
- [12] A. Rényi, "On Measures of Dependence," *Acta Math. Hung.*, Vol. 10, pp. 441-451, 1959.
- [13] S. Boyd and L. Vandenberghe, *Convex Optimization*, Cambridge University Press, 2004.
- [14] T. M. Cover, A. El Gamal, M. Salehi, "Multiple Access Channels with Arbitrarily Correlated Sources," *IEEE Transactions on Information Theory*, Vol. IT-26, pp. 648-657, Nov., 1980.
- [15] R. Ahlswede, and P. Gács, "Spreading of Sets in Product Spaces and Hypercontraction of the Markov Operator," *The Annals of Probability*, Vol. 4, No. 6, pp. 925-939, Dec. 1976.
- [16] V. Anantharam, A. Gohari, S. Kamath, C. Nair, "On Maximal Correlation, Hypercontractivity, and the Data Processing Inequality studied by Erkip and Cover", arXiv: <http://arxiv.org/abs/1304.6133>
- [17] H.S. Witsenhausen, "On sequences of pairs of dependent random variables," *SIAM Journal on Applied Mathematics*, vol. 28, no. 1, pp. 100-113, Jan. 1975.
- [18] H. L. Van Trees, *Detection, Estimation, and Modulation Theory, Part I*, Wiley Interscience, 2001.